

Internet Sheriff Version 5.2 Release Notes

June 2009



Internet Sheriff Technology Ltd
www.isheriff.com

Table of Contents

1. New features	3
2. Upgrading from previous versions	4
a. Upgrading from v4.x or v5.0	4
i. [Optional] Backup configuration data.....	4
ii. [Optional] Backup logs, stats and spool	4
iii. Remove the v4.x or v5.0 package	5
iv. [Optional] Clean up any remaining files	5
v. [Optional] Restore configuration data	5
vi. [Optional] Restore logs, stats and spool	5
vii. Install the v5.2 package	5
viii. Convert stats files	5
b. Upgrading v5.2.....	6
i. [Optional] Backup configuration data.....	6
ii. [Optional] Backup logs, stats and spool	6
iii. Upgrade the v5.2 package	6
3. Bugs fixed	7
a. Version 5.2.1:.....	7
b. Version 5.2.2:	7
c. Version 5.2.3:.....	8
d. Version 5.2.4:	9
e. Version 5.2.5:	9
f. Version 5.2.6:	9
g. Version 5.2.7:	10
h. Version 5.2.8:	10
i. Version 5.2.9:	10
j. Version 5.2.10:.....	10

I. New features

The following major new features have been released in Version 5.2:

Multiple time zone support

Individual realms and workgroups may be assigned time zones relative to their locality in order for filters and reports to be scheduled more accurately. This setting is independent of the actual system clock time allowing for servers to be logically or physically located in chronographically independent locations. Time-of-day filter rules are applied according to the individual time zone offset of the realm rather than the time zone of the server. Reports are automatically adjusted to offset the time axis to show the data in the local time zone context for the particular user group requested.

Clustering

Clustering provides the ability to maintain an array of servers as a single cluster with centralised management. Distribution of filter policy configuration data is fully automated, greatly reducing systems management overhead. Changes made to the policy on a live running system are automatically propagated on demand to every server in the cluster, providing a consistent filtering experience for end-users. Statistics from all machines are automatically aggregated to provide system-wide reports for the entire user-base.

In addition to the system management interfaces (Web and CLI), the filter policy configuration files may also be edited by any external means (vi, scripts, PHP, web portals etc) and the changes will be automatically detected and propagated to the entire cluster, even if a server is offline at the time.

Database support for reporting

Reporting data may now be optionally stored in a database for greater scalability and efficiency. The use of a database backend in larger installations provides for more uniform end-user response times when generating reports. As for a non-database installation, reports may be generated on demand and will display near real-time data, or may be scheduled to run automatically in batch mode. This option also allows for access to the raw data via SQL, third party tools, or custom database access routines.

Presently the MySQL database is supported natively. Other databases may become available in future versions. The original iSheriff proprietary data file format is still supported and is recommended for smaller installations or where simplicity is desired.

Extended custom email lists

Individual realms and workgroups may now be assigned an unlimited number of private custom email lists not visible to other realms. These lists may then be used for filtering purposes as allow lists, or deny lists or with other actions as appropriate.

Group alias quarantine recipients

Quarantine notices directed to a group or list alias (e.g. info@, sales@ etc) are now able to have a single nominated recipient specified. This overcomes the issue of multiple users receiving the same notification for a single mailbox, reducing unwanted notices and administration overheads.

Email grey-listing

An enhancement to the effectiveness of email filtering of spam and viruses, grey-listing postpones delivery of suspect emails at the SMTP communication layer. This approach is highly effective and blocks spam attacks at the earliest possible point during delivery, greatly reducing the load and volume of spam for processing by further deep inspection filters. Spam outbreaks can be reduced in volume by as much as 90% by this means alone.

2. Upgrading from previous versions

a. Upgrading from v4.x or v5.0

Internet Sheriff v5.2 configuration data is not fully compatible with v4.x or v5.0 configuration data, however the package contains a tool for converting v4.x or v5.0 configuration data into the v5.2 format.

N.B The v4.x or v5.0 package must be removed prior to installing v5.2. All configuration data, reporting data, logs and the mail spool may be kept, however on some platforms the package removal process may erase these files, so it is recommended that all data be backed up for later restoration prior to upgrading.

If you do not wish to keep any previous data, perform only steps (ii) and (iii). If you wish to merge the configuration, reporting data, logs and mail spool from the previous installation, then proceed through all steps as set out below.

It is recommended that you record offline details of your workgroups, policies and rules, custom lists and also SMTP and HTTP configuration details. Should anything malfunction during the upgrade process these can always be manually re-entered, if records are kept.

N.B Prior to backing up, be sure to stop any currently running Sheriff process.

i. [Optional] Backup configuration data

Refer to the relevant v4.x or v5.0 version of *Internet Sheriff User Guide Part I Installation and System Management* as to the file system path to the following folder:

Solaris/Linux: /opt/Sheriff/etc

MacOSX: /Library/Sheriff/etc

Backup this folder using `tar` or other preferred archiving utility, for example:

```
% cd /opt
% tar -cf /tmp/etc.tar Sheriff/etc
```

ii. [Optional] Backup logs, stats and spool

Refer to the relevant v4.x or v5.0 version of *Internet Sheriff User Guide Part I Installation and System Management* as to the file system path to the following folders:

Solaris/Linux: /var/opt/Sheriff

MacOSX: /var/Sheriff and /Library/Logs/Sheriff:

/logs/

/stats/

/spool/

Backup each of these folders using `tar` or other preferred archiving utility, for example:

```
% cd /var/opt/Sheriff/logs
% tar -cf /tmp/logs.tar *
% cd ../stats
% tar -cf /tmp/stats.tar *
% cd ../spool
% tar -cf /tmp/spool.tar *
```

iii. Remove the v4.x or v5.0 package

Refer to the relevant v4.x or v5.0 version of *Internet Sheriff User Guide Part I Installation and System Management* for the appropriate de-installation command. For example:

```
% pkgrm Sheriff
```

iv. [Optional] Clean up any remaining files

Refer to the relevant v4.x or v5.0 version of *Internet Sheriff User Guide Part I Installation and System Management* as to the installation file system paths. Binaries and temporary folders that may have been left behind by the package removal process may be safely removed.

v. [Optional] Restore configuration data

At this point you may wish to restore the old v4.x or v5.0 configuration data if the packaging removal system has erased it (e.g. Solaris). When the v5.2 package is added in the next step, it will automatically convert the old data into the new format. To restore the `etc` folder backed up in step (i):

```
% cd /opt
% tar -xf /tmp/etc.tar
```

vi. [Optional] Restore logs, stats and spool

At this point, you may wish to restore the old v4.x or v5.0 data if the packaging removal system has erased it. Restore the `logs`, `stats` and `spool` folders archived in step (ii):

Continuing with the `tar` example above, we would restore as follows:

```
% cd /var/opt/Sheriff/logs
% tar -xf /tmp/logs.tar
% cd ../stats
% tar -xf /tmp/stats.tar
% cd ../spool
% tar -xf /tmp/spool.tar
```

The Sheriff process may now be restarted and configured.

vii. Install the v5.2 package

Refer to *Internet Sheriff User Guide Part I Installation and System Management Version 5.2* for full installation directions.

If proceeding with the next step, be sure to stop any running Sheriff process.

viii. Convert stats files

Convert existing v4.x or v5.0 `stats` files into v5.2 format as follows:

```
% /opt/Sheriff/bin/estat_stat_convert
% cd var/opt/Sheriff/
% mv stats stats.old
% mv converted_stats stats
```

b. Upgrading v5.2

It is recommended that you record offline details of your workgroups, policies and rules, custom lists and also SMTP and HTTP configuration details. Should anything malfunction during the upgrade process these can always be manually re-entered, if records are kept.

N.B Prior to backing up, be sure to stop any currently running Sheriff process.

i. [Optional] Backup configuration data

Refer to the relevant v5.2 version of *Internet Sheriff User Guide Part I Installation and System Management* as to the file system path to the following folder:

Solaris/Linux: /opt/Sheriff/etc

MacOSX: /Library/Sheriff/etc

Backup this folder using tar or other preferred archiving utility, for example:

```
% cd /opt
% tar -cf /tmp/etc.tar Sheriff/etc
```

ii. [Optional] Backup logs, stats and spool

Refer to the relevant v5.2 version of *Internet Sheriff User Guide Part I Installation and System Management* as to the file system path to the following folders:

Solaris/Linux: /var/opt/Sheriff

MacOSX: /var/Sheriff and /Library/Logs/Sheriff:

/logs/

/stats/

/spool/

Backup each of these folders using tar or other preferred archiving utility, for example:

```
% cd /var/opt/Sheriff/logs
% tar -cf /tmp/logs.tar *
% cd ../stats
% tar -cf /tmp/stats.tar *
% cd ../spool
% tar -cf /tmp/spool.tar *
```

iii. Upgrade the v5.2 package

Installation of the v5.2 package will automatically perform an upgrade. Refer to *Internet Sheriff User Guide Part I Installation and System Management Version 5.2* for full installation directions and the appropriate installation command. For example:

```
% pkgadd Sheriff_5.2.0.solaris_sparcv9.pkg
```

3. Bugs fixed

The following bugs have been fixed.

a. Version 5.2.1:

Bug No	Description
1337	Default filter policies do not block PROXYAVOIDANCE category
1367	Authorised emails use wrong filter policy
1369	Support for paged LDAP queries for large ADS lookups
1370	Data missing from long term reports
1371	Assertion failed: <code>conn->c_data_in != NULL</code>
1372	Assertion failed: <code>callback_func</code>
1373	Email filter tab does not show configured policy properly for non-admin user
1374	Email filter configuration generates duplicated email addresses/domains
1376	Email addresses truncated in SVG reports
1377	Ability to override the base URL in block and coach pages
1380	Duplicate reporting data in SVG reports
1386	Deleting a realm causes filter pod to fault upon restart
1387	Empty reports when in database mode

b. Version 5.2.2:

Bug No	Description
1375	Excessive memory consumption when running large volumes of email
1393	Adding quarantined email message sender to personal whitelist fails
1395	Crash when running reports with very large volumes of data
1405	A realm with no user definition implies all users, which interferes with realms that explicitly define all users
1411	Assertion failed: <code>!(ACOUNT_SIG(a) & ((flags) & ACOUNT_SIGMASK))</code> , file <code>mceAttach.c</code> , line 256
1413	Report line limit setting does not change the report line limit

c. Version 5.2.3:

Bug No	Description
I397	Excessive CPU and asserts on Debian 4.0
I414	Accurate statistics required for cancelled downloads
I416	Failed SSL connections may cause engine to spin
I418	Crash in statistics compaction (memory corruption)
I419	Assertion failed: stream_ep->conn == NULL
I430	Email greylist timeout setting not actually honoured
I433	Direct access to report for a single user, group, website or email address directly
I439	Exporting tabular reports to CSV file gives Javascript error in IE
I440	Insertion of Sheriff footer into quoted-printable encoded html body parts may enlarge fonts
I441	Report platform, OS version and hardware summary at startup
I444	Spam with garbage RCPT address can crash greylisting
I446	Per-message quarantine notifications have blank from address
I447	Custom model that can search for filenames in the URL path
I448	Auto-add sender to personal whitelist on quarantine release

d. Version 5.2.4:

Bug No	Description
I400	Removal of the obsolete Management Users tab on the Realm page in the configuration screen
I429	Manually initiated stats aggregation job can be overrun by cron job
I431	Missing icons in category component edit form
I434	Large reports take too long to generate
I445	Very large reports drain CPU and may eventually crash the system
I454	Tag footer append breaks verification of digitally signed messages
I457	Additional coach page template variable for the session token
I459	SMTP EHLO response should not include STARTTLS if already using SSL
I462	Source IP addresses in SMTP transport log may be truncated
I468	Report cache housekeeping may cause crash
I473	Unparseable emails in outbound message queue cause crash loop
I475	Enabling MySQL reporting fails when alternative Unix socket file is used
I476	mce_sprintf() causes buffer overruns
I480	Multiple issues with report generation and stats processing: <ul style="list-style-type: none">• Per-user reports may show duplicate data• Database report settings sometimes fail to save when modified via the WMI• Improved report data caching and memory usage• Aggregation runs under local timezone instead of GMT• Fixed the sorting on certain tabular reports

e. Version 5.2.5:

Bug No	Description
1417	Too many open files error when using upstream proxy
1470	Database reporting setup creates a dbrmysql.conf that causes the DB-report pod always to abort

f. Version 5.2.6:

Bug No	Description
1482	Fixed deadlock issue with LDAP lookup test screen

g. Version 5.2.7:

Bug No	Description
1412	LDAP user authentication fails intermittently
1466	WMI user with same roles as admin not able to generate any reports

h. Version 5.2.8:

Bug No	Description
N/A	Not released

i. Version 5.2.9:

Bug No	Description
1421	Nightly automated report tasks may fail to run
1485	Assertion '!carrier->msg_head' failed
1488	FTP downloads may fail when using upstream proxy

j. Version 5.2.10:

Bug No	Description
1491	Anti-spam updates fail to run on Linux installations