


5.3 Privacy Settings and System Logs

1. Privacy Settings



Present section was formerly known as "Data Retention" and has been updated and renamed because of deep improvements in PrivateServer Data Management.

Privacy Settings are EVSS feature about archiving and storing policies for some historical data.

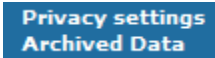


figure 1. Menu access to the Data Retention

You can access **Privacy Settings** and its counterpart **Archived Data** by menu entries shown in [figure 1. Menu access to the Data Retention](#) under "**SERV ER CONFIGURATION**".

Privacy Settings are used to manage data kept into PrivateServer operational database:

- Data Retention: define for how much time data are kept
- Data masking: define if and which information are stored

1.1. Setup of Privacy Settings: Data Retention Policy

Privacy Settings are split in two different subsections called **Data Retention Policy** and **Data Masking**.

Data Retention Policy

Data Type	Enabled	Export to file	Period Duration	Period/s Online
Web Session	False	False	YEAR	1
Call Detail Record	False	False	YEAR	1
SIP Session	True	False	MONTH	1
System Event	True	False	MONTH	1
Security Event	True	False	MONTH	1
privateserver.messaging.Message	True	False	MONTH	1

Data masking

Call detail record:

Disabled


Secure message:

Disabled


Update

figure 2. Data Retention Policy list

Data Retention Policy is about keeping historical data in database, exporting them to local filesystem per your timetable. You can configure retention policies for all historical data managed by the appliance, which are listed in [figure 2. Data Retention Policy list](#). In the same list you can also read if retention is **Enabled**, how many periods (**Period Online**) you want to keep online in database and your period unit (**Period/s Online**: Day, Week, Month, Year).



The data involved in the process are deleted from internal database and exported on local file system for archival.



If you need to understand the data stored in each Data Type, please refer to the [logging](#) section of the present manual.

By clicking on each row's **Data Type** you can access to specific Policy form that let's you edit Data Retention behaviour.

Edit Data Retention Policy

Data Type:

Web Session

Enabled:

☐

Export to file:

☐

Period Duration:

YEAR

Period/s Online:

1


 Update

figure 3. Data Retention Policy editor

Such form is shown as an example in [figure 3. Data Retention Policy editor](#). Using the mentioned form you can:

- enable the Data Retention (**Enabled** checkbox)
- enable Export to file if you want data to be retained otherwise with un-checked box, data will be deleted from database and not written to file.
- select the period unit (Day, Week, Month, Year)to be kept on-line (**Period Duration**)
- choose how many periods you want to keep online (**Period/s Online**)

1.2. Setup of Privacy Settings: Data Masking

Data Masking is about the way informations are recorded.

Data masking

Call detail record:

Disabled

Secure message:

Do not archive

Masked out

Disabled


 Update

figure 4. Data Masking options

Three options are available for logs about Calls and Secure Messages:

1. **Do not archive:** PrivateServer won't keep trace of any record at all. Exception is for enqueued Secure Messages to be delivered: they are shown in web console as masked events and they are deleted as soon as delivered to recipient.
2. **Masked out:** mask all sensitive data replacing them with "XXX". You just get time and duration of calls and trace of message delivery but you cannot tell who's who for both sender and receiver or caller a callee.
3. **Disabled:** no masking is applied and events are kept in their original form.

Whichever Data Masking policy is configured, Data Retention policy applies: it is possible to have secure messages masked and configure one week data retention policy, to automatically delete them, as soon as they are not useful anymore for support needs to end-users.

Data Masking changes type of data that are going to be stored (if you chose to store them at all).

2. Retrieve the Data Archives

As said in the previous paragraph (4.0.3.2), there are two left menu entries to manage the Data Retention feature (see [figure 1. Menu access to the Data Retention](#)). If you want to access to the stored archives just press the **"Archived Data"** link.

Data Archive List


















Name	Timestamp	Size		
sessionLogEntry-2013-09-16-20130922040000.zip	2013-09-22 03:00:14.000	655.188 kilobytes		
cdr-2013-09-16-20130922040000.zip	2013-09-22 03:00:00.000	2.184 kilobytes		
sessionLogEntry-2013-09-09-20130915040000.zip	2013-09-15 03:00:17.000	645.887 kilobytes		
cdr-2013-09-09-20130915040000.zip	2013-09-15 03:00:00.000	1.858 kilobytes		
sessionLogEntry-2013-09-02-20130908040000.zip	2013-09-08 03:00:16.000	627.813 kilobytes		
cdr-2013-09-02-20130908040000.zip	2013-09-08 03:00:00.000	1.982 kilobytes		
sessionLogEntry-2013-08-26-20130901040000.zip	2013-09-01 03:00:32.000	615.472 kilobytes		
cdr-2013-08-26-20130901040000.zip	2013-09-01 03:00:02.000	3.187 kilobytes		

figure 5. Data Archive List


The "Data Archive List" is shown in the page body (see [figure 5. Data Archive List](#)). Each archive row shows its **Name**, its **Creation Timestamp** and its **Size** (all the columns are pretty self explaining).

The last two columns shows two icons: the first one is for downloading the archive, the second one is for deleting it.

 It's possible to download the archive also by clicking on its name

2.1. Data Archives and Secure Messaging

You can just download a CSV view of Secure Message transport data, such as sender, recipient, acceptance date, delivery status.

 Secure Messages payload is **never** saved. As soon as Message has been delivered, its payload (aka Message content) is deleted from PrivateServer's data storage

3. Delete Data Archives

If you choose to delete the archive, press the last column icon.

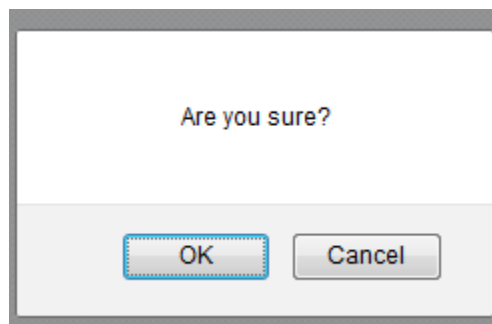



figure 6. The confirmation pop-up window

A confirmation is requested (see [figure 6. The confirmation pop-up window](#)). If you approve the action then the archive is removed from both the list and the hard disk of the appliance.

 **Point of no return action!**
Please be aware that this action isn't undoable! Once confirmed the deletion, the archive is lost forever!

4. System's logs

In addition to historical data collected in internal database, the two main PrivateServer 's components can log debug information in log files.

They main components are:

- Secure Voip Engine
- Web Console

Both of them use default system locations (specifically directory `/var/log`) to store their logs. PrivateServer saves only the last week of these files and rotates them on a daily base. Rotate operation implies both deletion for files older than one week and archiving in `.zip` format for the most recent ones. All the log files are labelled by timestamp of the rotation.

5.2 MONITORING