[New Install From CD or ISO](#_gzghp52zy4i2)

[Upgrade from CD or ISO](#_m17banm8b0tw)

[Upgrade from upgrade script](#_loh4538ftln1)

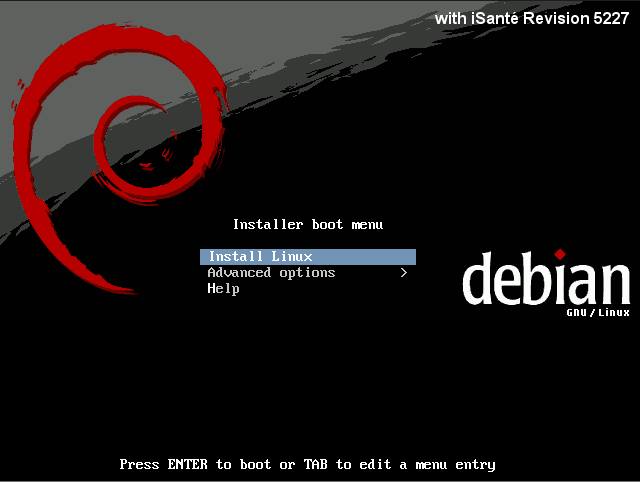
[Recover using backup](#_5q9qinm5vvlr)

[Recovering a corrupted MySql installation](#_jtqkdmji68qx)

[Move an existing ASP site in-country/Recover with a consolidated site gz file](#_bibn1x3avfa6)

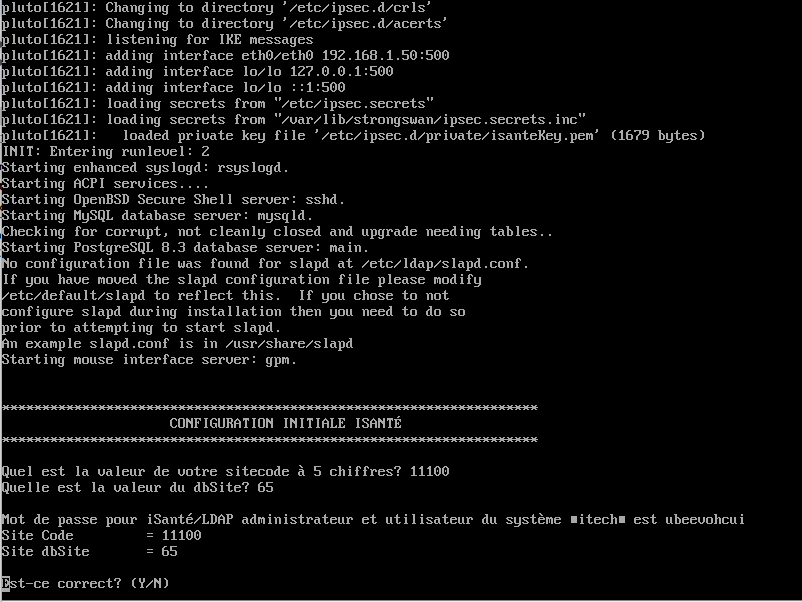
# New Install From CD or ISO

WARNING: This process will completely erase the system's hard drive.

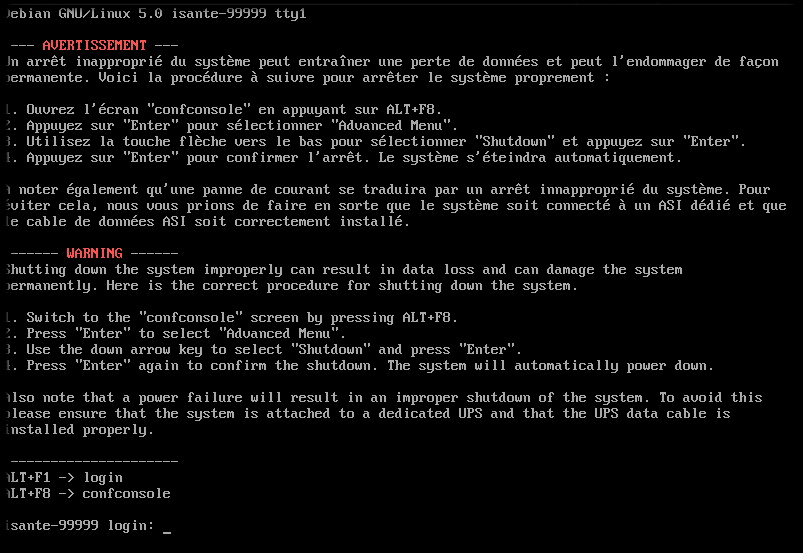
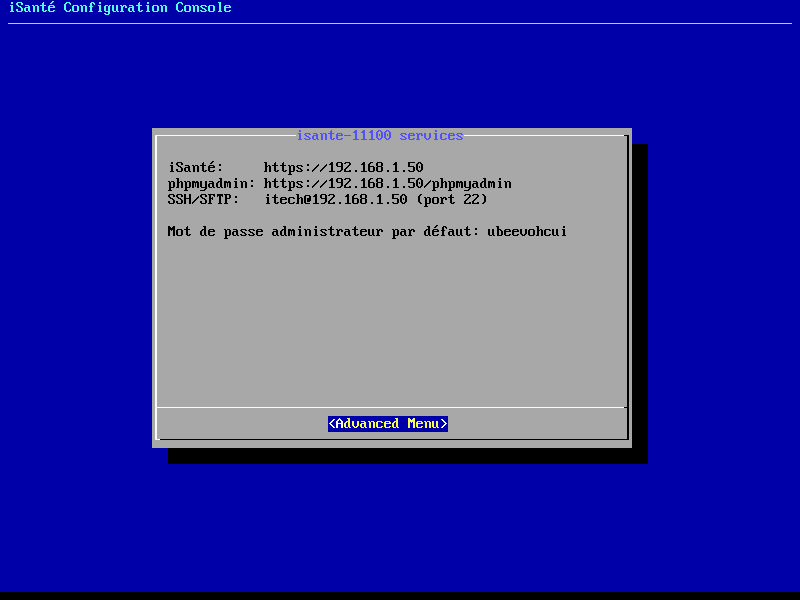
1. Boot from the CD.

2. Select "Install Linux" from the boot menu.

3. The installer will ask if it is okay to format the system's hard drive, install Debian and reboot the machine (10-20 minutes).

4. During the first boot you will be asked a few questions about dbSite and siteCode values for the installation.

After that the system will be fully setup and ready to use. The console screen is displayed:

Notice that since the password for the itech user is randomly generated, a reference on the console reminds the user that ALT+F8 will switch the user to the configuration console, which provides the password value:

# Upgrade from CD or ISO

1. Boot the machine normally, logging in as the itech user

2. Insert the CD and issue the command `mount /cdrom`

3. Run the command `sudo sh /cdrom/simple-cdd/upgrade`

4. A prompt will show the version number of the currently installed version and the version being upgraded to. Press ENTER here to proceed with the upgrade. (30-45 minutes)

5. The system may reboot when the upgrade is done. You will need to remove the CD at this point.

If you have the .iso image on a hard drive or USB drive you can use this alternative step 2:

2. Issue the command `sudo mount <path\_to\_.iso\_image> /cdrom -o loop`

# Upgrade from upgrade script

WARNING: This method requires an active Internet connection.

1. Boot the machine normally and log in as the itech user.

2. Copy the update-package.sh.gz file from almond.cirg.washington.edu onto the system.

3. Unzip the update package script

gunzip update-package.sh.gz

4. Issue the command `sudo sh <path\_to\_update-package.sh\_file>`

5. If additional system software is required for this upgrade a prompt will appear saying what needs to be installed. Pressing ENTER here will download the needed software from the central Debian repository. The upgrade will abort if there is no Internet connection.

6. A prompt will show the version number of the currently installed version and the version being upgraded to. Press ENTER here to proceed with the upgrade. (30-45 minutes)

7. The system may reboot when the upgrade is done.

# Recover using backup

The syntax for doing an iSanté recovery [as of 12.3] is:

sudo sh /var/www/isante/support/restore-db-linux.sh <backup\_file> [<encryption\_key>]

The restore script does the following:

* restores the site configuration information
* restores the underlying database
* restores the LDAP directory
* if necessary, upgrades the restored database to the installed version if iSanté

The encryption\_key argument is optional in the sense that if the damaged database is still working sufficiently to be able to provide the key, the restore will fetch it from the damaged database.

Otherwise the key must be provided unless the backup file was made by a release older than 12.3. Backup files from previous versions can still be used for recovery; backups done with 12.3 or greater append “E\_” to the filename as an indication that they are encrypted.

If the encryption key isn’t available from the existing database and was not stored somewhere safe, it can still be recovered. iSanté replicates the generated key to the consolidated databases. To obtain the encryption key from a consolidated database, log in to a consolidated database, go to Administration → Requête, and enter the following query:

select substr(eventParameters, 40,locate('\"}',eventParameters)-40)

from eventLog where dbsite= <enter\_dbsite\_here> and eventLog\_id in (

select max(eventLog\_id) from eventLog

where eventtype = 'configChange' and

eventParameters like '%backupEncryptionKey%')

# Recovering a corrupted MySql installation

Please read the article here:

<http://dev.mysql.com/doc/refman/5.1/en/forcing-innodb-recovery.html>

Jim used this command line to recover an installation sufficiently to recover the backup encryption key:

/usr/bin/mysqld\_safe --defaults-file=/etc/mysql/my.cnf --console

--innodb\_force\_recovery=6

Be aware that using any of the values for --innodb\_force\_recovery (0-6) renders the database unusable except for SELECT operations to dump tables. This is a last resort for getting the encryption key if it is not available from a consolidated site.

# Move an existing ASP site in-country/Recover with a consolidated site gz file

1. Establish a "cut-off date," which is the last day that the site enters data to the ASP server. This should be negotiated with the on-site clinical personnel.

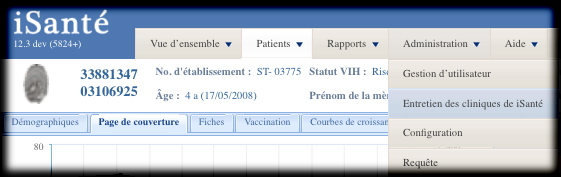
2. One day after the cut-off date, on the Port Au Prince consolidated (coordinating) server:

A. Log on to the PaP site:

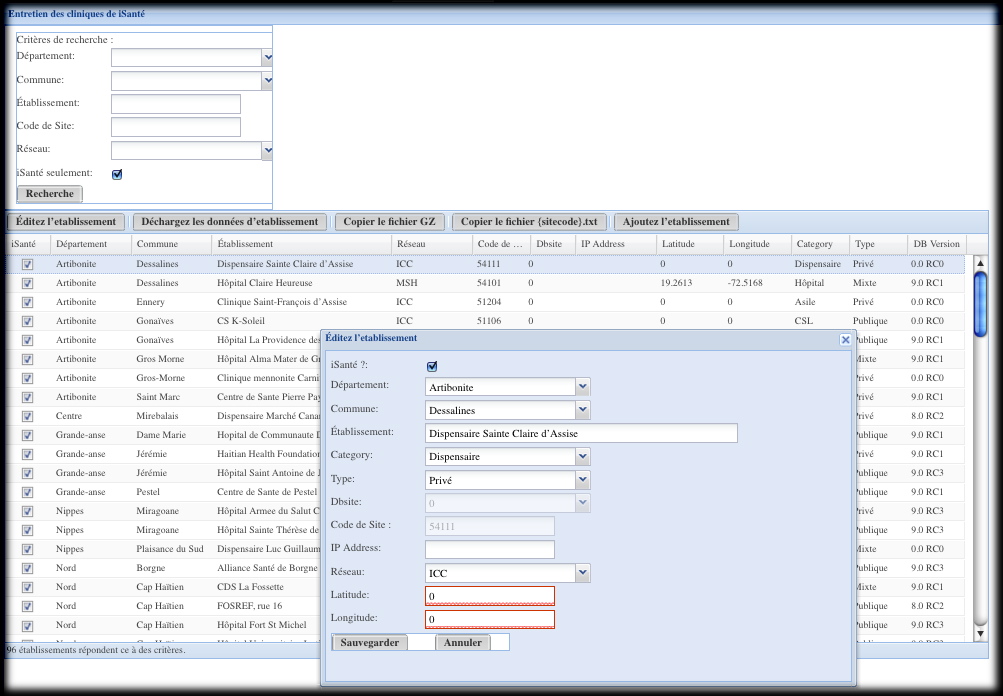
<https://isante.ugp.ht/consolidatedId/isante>

Verify that all work done as of the cut-off date has been replicated to the consolidated server. If not, wait another day.

B. Search for the site using the menu item ***Entretien des cliniques de iSanté*** on the consolidated server:



C. Select the site and assign additional site attributes with the button **Éditez l'etablissement**. In particular, it is required that you select a **dbsite** value for in-country sites. Make note of **sitecode** and the selected **dbsite** value and fill in the site’s **hostname** and **IP address**, if known.



D. Unload the site’s data with the button **Déchargez les données d'etablissement**. The data file is automatically placed on the server here:

/var/backups/itech/unloads/

After a successful unload, the above directory should contain the following files:

{sitecode}errors.txt contains any errors during the unload (should be zero size)

{sitecode}.txt summarizes the data unloaded

{sitecode}.csv.gz contains the site’s data

where {sitecode} represents the actual **sitecode** value (i.e. HUEH is 11100) for the site.

{sitecode}.csv.gz will be used to load the site’s new server in step 6) below.

3. Install the site's on-site server.

4. Install iSanté and OpenELIS as specified in their respective installation guides, providing the **sitecode** and **dbsite** values when asked. **IMPORTANT: when moving an ASP site in-country, it is essential that the most recent version of iSanté be installed. If this is not done, there is the possibility of data loss.** Obtain the most recent iSanté version here:

haiti01@almond.cirg.washington.edu

5. Copy the unloaded {sitecode}.csv.gz file from the consolidated server location above so that it can be applied to the new server. You can copy the {sitecode}.csv.gz file to your client computer using the **Copier le fichier GZ** button, but ***please wait long enough be sure it is completely unloaded*** before copying.

For comparison purposes later, also copy the unload statistics file {sitecode}.txt, using the button **Copier le fichier {sitecode}.txt**. This file will be empty until the gz file is completely written to disk.

6. While logged on to the new server, load the new server with the site’s data:

sudo sh

cd /var/www/isante/replication

perl updateTarget.pl --file {sitecode}.csv.gz > {sitecode}.txt 2> {sitecode}errors.txt

This load process could take some time, particularly for a site with more than 200 patients.

7. Verify that the load was successful by comparing the {sitecode}.txt file generated on the consolidated site in step 2.D) with the {sitecode}.txt file generated in step 6).