Security of Information and Communication Systems

# INSTALLATION

Table of contents

1. Introduction

This document describes the installation procedure of the ALCASAR portal. It is supplemented with three other documents : the presentation document, the operating instructions document and the technical document.

If you already have a working version of ALCASAR and you want to upgrade it, please refer to the operating instructions document (chapter « update »).

ALCASAR can be installed on a standard computer with two Ethernet network cards. The first one (eth0) is connected to the Internet Service Provider's equipment. The second one (eth1) is connected to the switch used to service the network consultation computers.

By default, the IP address of this second network card is : 192.168.182.1/24. This allows to have a class C network (254 equipments). This network addressing plan can be modified during the installation stage. For all equipment of consultation network, ALCASAR is the DHCP server, the DNS server, the network time server and the default router (gateway). **Thus, on this network, there must be no other DHCP server and gateway** (check your wifi access points).
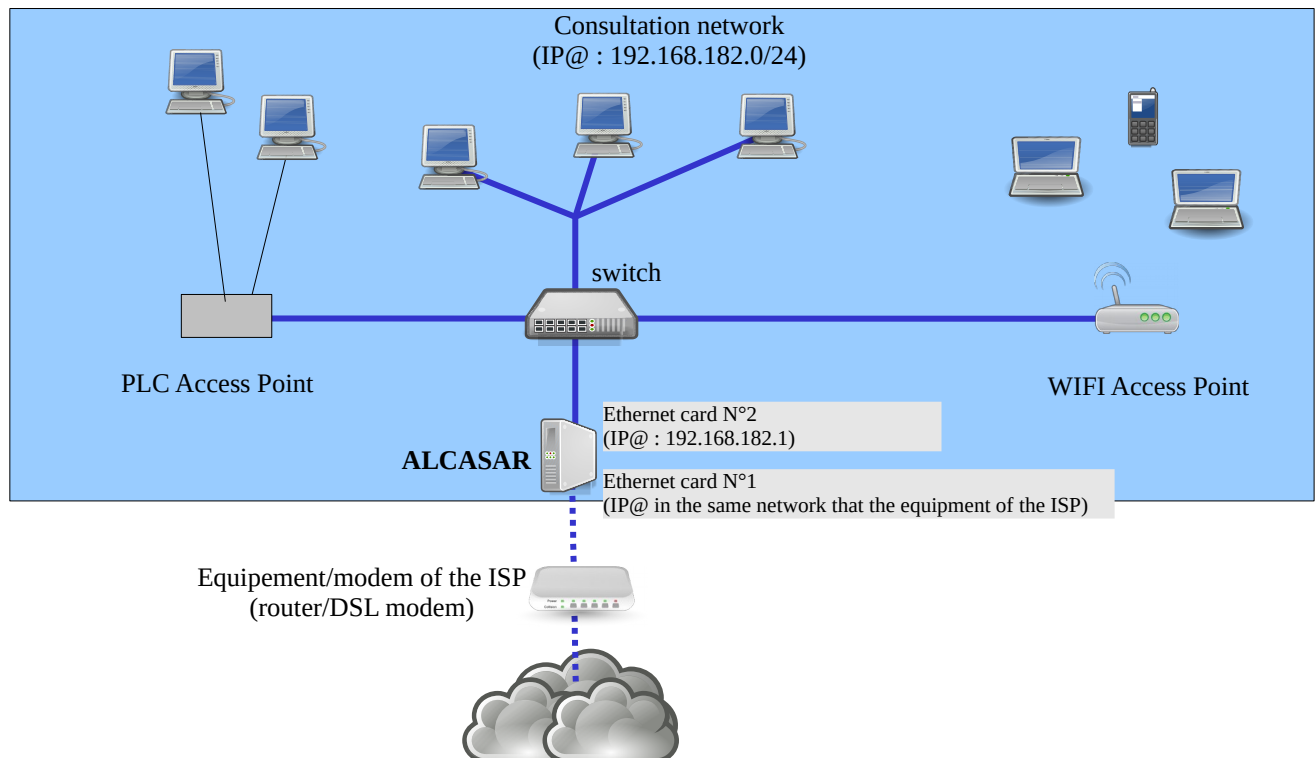
Example with default class C network (254 equipments)
- IP address of ALCASAR : 192.168.182.1/24
- Maximum number of equipment on the consultation network : 253
- Network settings of equipment :
  - available IP addresses : from 192.168.182.2 to 192.168.182.254 (static or dynamic)
  - subnet mask : 255.255.255.0
  - IP address of the DNS server and of the default gateway : 192.168.182.1 (IP address of ALCASAR)
  - DNS suffix for equipment with static IP address : "localdomain"

Example with a class B network (65534 equipments)
- IP address of ALCASAR : 172.16.0.1/16
- Maximum number of equipment on the consultation network : 65533
- Network settings of equipment :
  - available IP addresses : from 172.16.0.2 to 172.16.255.254 (static or dynamic)
  - subnet mask : 255.255.0.0
  - IP address of the DNS server and of the default gateway : 172.16.0.1 (IP address of ALCASAR)
  - DNS suffix for equipment with static IP address : "localdomain"

Even if it is possible to define a class A network, you shouldn't do it because the embedded DHCP server will have to manage over than 16 millions of IP addresses. The management of such volume of addresses would spend too much memory.

2. **Installation**

The installation of the portal consists of two steps. The first one is the installation of a minimalist Linux operating system based on Mageia 4.1. The second step installs and configures all the components of ALCASAR.
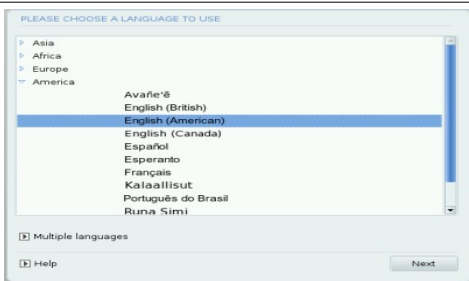
2.1. Hardware requirement

ALCASAR only requires one standard desktop computer with two network cards and a hard drive with a capacity of at least 100 Go in order to be able to store logs related to connections tracing. ALCASAR includes several optional filtering systems (network protocols, URL, IP addresses, domain names and antimalware). If you decide to enable these filtering systems, it is recommended to install at least 8GB of RAM in order to ensure an acceptable processing speed (ALCASAR loves the RAM ;-))

⚠ In case of using a Virtual Machine (VM) : be sure that the size of the hard drive **isn't less than 25G.**
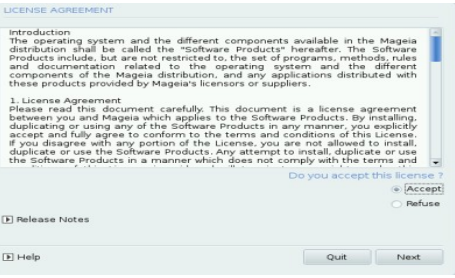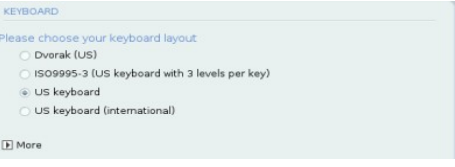
2.2. Installation of the system
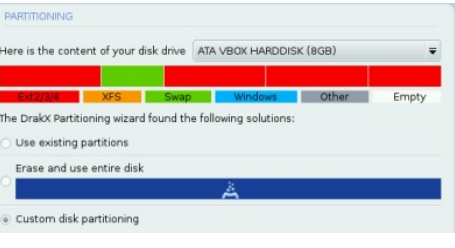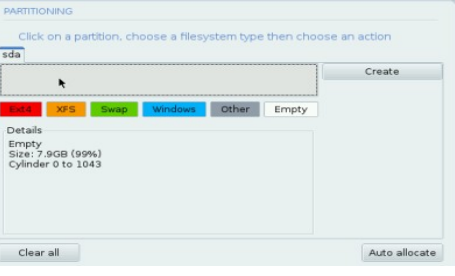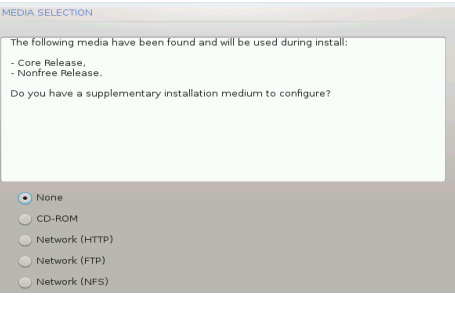
The installation procedure of the operating system is the following (estimated time : 6') :
- get the Mageia 4.1 ISO image file in double architectures (32 and 64 bits) : « mageia-4.1-dual-DVD.iso » (1 GB). This ISO image is available on ALCASAR website as well as on several mirror sites of Mageia. For example :
  - http://www.mirrorservice.org/sites/mageia.org/pub/mageia/iso/4.1/
  - http://distrib-coffee.ipsl.jussieu.fr/pub/linux/Mageia/iso/4.1/
- burn this ISO image file on a DVDROM or create a bootable USB flash drive[1]. You can also use a external USB disk which simulate a bootable device (ex : zalman zm-ve300 or 400).
- configure the BIOS settings to unset the "Secure Boot" option, to set the date and time and to enable booting from the CD or USB flash drive. At the end of the installation, configure, once again, the BIOS settings to only boot from the hard drive ;
- insert the CD-ROM or the USB flash drive, reboot the computer and follow the instructions bellow :
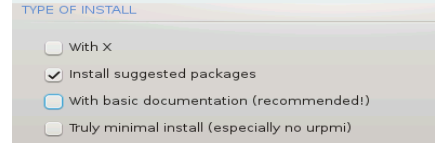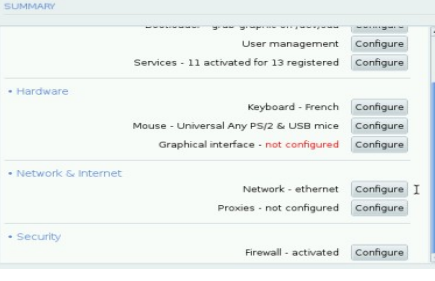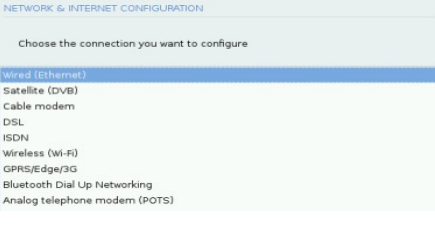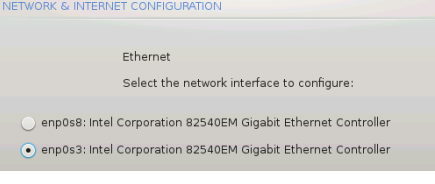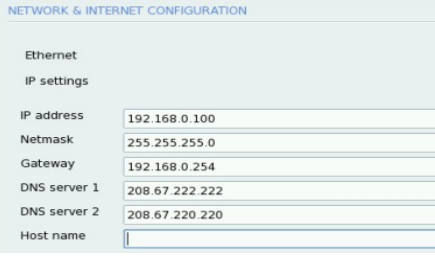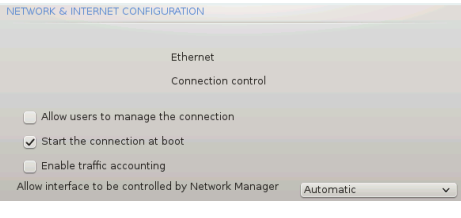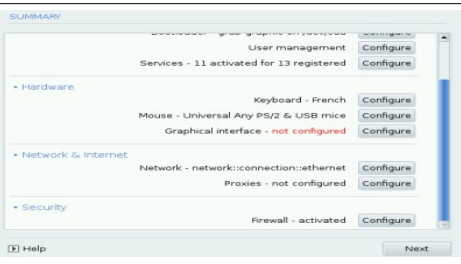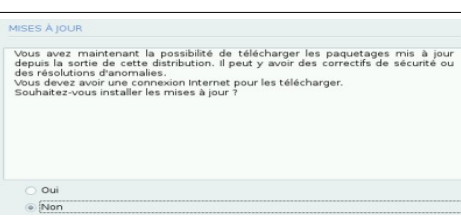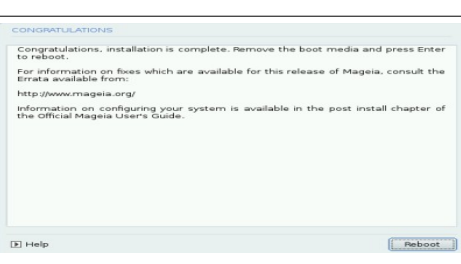
Screen display	Comments	Actions to achieve
	After starting the computer, this screen is displayed. * If the graphical mode doesn't work, you have to configure the BIOS settings to allocate more than 2MB of shared memory for the graphics card.	Select "Install Mageia 4".
		Select your language.

---

1 Two solutions are used to create a bootable USB flash drive :
- in graphical mode you can use "usbdumper" (Windows) or "isodumper" (Linux)
- in console mode on Linux, plug the USB flash drive and get the name of the device with the "*fdisk -l*" command (an USB flash drive is usually "/dev/sdb" or "/dev/sdc"). Run the command : "*dd   if=<name_of_ISO_image>   of=<name_of_usb_drive> bs=1M*".
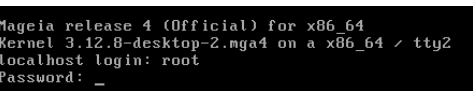
Screen display	Comments	Actions to achieve
LICENSE AGREEMENT		Accept the license agreement. Info : this license agreement explains that the installed software are free (GPL).
KEYBOARD Please choose your keyboard layout ○ Dvorak (US) ○ ISO9995-3 (US keyboard with 3 levels per key) ◉ US keyboard ○ US keyboard (international) ▶ More		Choose your keyboard layout.
PARTITIONING Here is the content of your disk drive ATA VBOX HARDDISK (8GB) Ext2/3/4 XFS Swap Windows Other Empty The DrakX Partitioning wizard found the following solutions: ○ Use existing partitions Erase and use entire disk ◉ Custom disk partitioning	The hard disk partitioning will be adapted to the needs of ALCASAR (see next step).	Select "Custom disk partitioning".
PARTITIONING Click on a partition, choose a filesystem type then choose an action sda Create Ext4 XFS Swap Windows Other Empty Details Empty Size: 7.9GB (99%) Cylinder 0 to 1043 Clear all Auto allocate	After removing all the partitions, create the following 5 partitions : • / : 4 GB • swap : keep the default size • /tmp : 4 GB • /home : 4 GB • /var : the rest of the hard drive (! **size bigger than 10G even on a virtual machine**).	Click on "Clear all". Then click on the area of the disk (sda) to create each new partition. Info : except the partition of swap, all the filesystem (FS) type are "Journalized FS : ext4".
Créer une nouvelle partition Taille en Mio : 4000 Type du système de fichiers : Journalised FS: ext4 Point de montage : / Chiffrer une partition Clé de chiffrement Clé de chiffrement (confirmation)	At the end of this operation, and depending on the size of your hard drive, the partitioning should look like this : sda / 3.9Gio /tmp 3.9Gio /home 2.9Gio /var 10Gio Ext4 XFS Swap Windows Autre Vide	- Create the root partition (/). Choose its size (4 Go) and its filesystem (ext4). Repeat this step for all the partitions. - Once the partitioning completed, click on "Done".
MEDIA SELECTION The following media have been found and will be used during install: - Core Release, - Nonfree Release. Do you have a supplementary installation medium to configure? ◉ None ○ CD-ROM ○ Network (HTTP) ○ Network (FTP) ○ Network (NFS)	For ALCASAR, it does not need any other media	Select "None" then click "Next"
MEDIA SELECTION Here you can enable more media if you want. Some hardware on your machine needs some non free firmwares in order for the free software drivers to work. You should enable "Nonfree Release" ☑ Core Release ☑ Nonfree Release		Leave the "Nonfree Release" media enabled then click "Next"

Screen display	Comments	Actions to achieve
PACKAGE GROUP SELECTION	Package group selection : ALCASAR only requires a very minimal install.	Select "Unselect All" then click "Next". <u>Info :</u> On Linux, a package is an archive file containing all the components of a software (binary files, help files, configuration files, etc.).
TYPE OF INSTALL ☐ With X ☑ Install suggested packages ☐ With basic documentation (recommended!) ☐ Truly minimal install (especially no urpmi)		Select only "Install suggested packages", then click "Next". The copy of the packages is launched. Estimated time : 2'
USER MANAGEMENT		Assign a password to the "root" account, then, create the "sysadmin" account and assign it a password.
SUMMARY	Configuration of Internet access	Click on "Configure" in "Network-ethernet" in the "Network & Internet" section.
NETWORK & INTERNET CONFIGURATION Choose the connection you want to configure Wired (Ethernet) Satellite (DVB) Cable modem DSL ISDN Wireless (Wi-Fi) GPRS/Edge/3G Bluetooth Dial Up Networking Analog telephone modem (POTS)		Select the type of Internet connection. In the case of use of an ISP broadband modem, choose "Wired (Ethernet)". <u>Info :</u> no test has yet been made on other types of Internet access.
NETWORK & INTERNET CONFIGURATION Ethernet Select the network interface to configure: ○ enp0s8: Intel Corporation 82540EM Gigabit Ethernet Controller ● enp0s3: Intel Corporation 82540EM Gigabit Ethernet Controller	For the moment, only the interface connected to the broadband modem of the ISP will be configured. The second interface, connected to the consultation network, will be configured later, during the installation of ALCASAR.	Select the interface to configure. <u>Tips :</u> Choose the interface with the smallest index. **Write the name of this interface on a paper.** <u>Info :</u> the names of interfaces are linked with the physical architecture of your PC. They could differ of the printscreen.
NETWORK & INTERNET CONFIGURATION Ethernet Please select your connection protocol. If you do not know it, keep the preselected protocol. ○ Automatic IP (BOOTP/DHCP) ● Manual configuration		Select "Manual configuration" <u>Info :</u> While it is possible to let this interface in "bootp/dhcp" mode, we recommended to configure it manually in static mode.
NETWORK & INTERNET CONFIGURATION Ethernet IP settings IP address 192.168.0.100 Netmask 255.255.255.0 Gateway 192.168.0.254 DNS server 1 208.67.222.222 DNS server 2 208.67.220.220 Host name	Example : • IP address : this address must be in the same subnet as the address of the broadband modem. • Netmask : 255.255.255.0 • Gateway : This is the address of the broadband modem • DNS 1 and DNS 2 :* • Host name : Leave this field blank	Enter the parameters of this interface * Enter the IP addresses of the DNS servers provided by your ISP. You can also use other DNS servers. Examples: • Free project "OpenNic" (see the web site to know the closest servers for you) • project "OpenDNS" (DNS1=208.67.222.222, DNS2=208.67.220.220) • google (DNS1=8.8.8.8, DNS2=8.8.4.4).

Screen display	Comments	Actions to achieve
NETWORK & INTERNET CONFIGURATION Ethernet Connection control ☐ Allow users to manage the connection ☑ Start the connection at boot ☐ Enable traffic accounting Allow interface to be controlled by Network Manager [Automatic ▾]		Select only "Start the connection at boot"
NETWORK & INTERNET CONFIGURATION Do you want to start the connection now? ○ Yes ◉ No	It is not necessary to start the connection now.	Select "No"
NETWORK & INTERNET CONFIGURATION Congratulations, the network and Internet configuration are finished.		Click on "Finish"
SUMMARY User management [Configure] Services - 11 activated for 13 registered [Configure] • Hardware Keyboard - French [Configure] Mouse - Universal Any PS/2 & USB mice [Configure] Graphical interface - not configured [Configure] • Network & Internet Network - network::connection::ethernet [Configure] Proxies - not configured [Configure] • Security Firewall - activated [Configure] ▶ Help [Next]		Click on "Next"
MISES À JOUR Vous avez maintenant la possibilité de télécharger les paquetages mis à jour depuis la sortie de cette distribution. Il peut y avoir des correctifs de sécurité ou des résolutions d'anomalies. Vous devez avoir une connexion Internet pour les télécharger. Souhaitez-vous installer les mises à jour ? ○ Oui ◉ Non	Security updates will be managed during the installation of ALCASAR.	Select "No" and click on "Next"
CONGRATULATIONS Congratulations, installation is complete. Remove the boot media and press Enter to reboot. For information on fixes which are available for this release of Mageia, consult the Errata available from: http://www.mageia.org/ Information on configuring your system is available in the post install chapter of the Official Mageia User's Guide. ▶ Help [Reboot]	The installation is finished	Click on "Reboot" Remove the CDROM or the USB flash drive Reconfigure the BIOS to boot only from the hard drive.

2.3. Installation of ALCASAR

Configuration of the network cards

Screen display	Comments	Actions to achieve
Mageia release 4 (Official) for x86_64 Kernel 3.12.8-desktop-2.mga4 on a x86_64 / tty2 localhost login: root Password: _	Disconnect the cables of the two network cards. Log in as root	
	Run the blinking of the LED of the network card configured previously. Stop the blinking	*ethtool -p enp0s3* *On this blinking interface, connect the cable linked to the ISP broadband modem (Internet access).* *<Ctrl> + c* Info : replace "enp0s3" with the name of the network card you've configured previously (see Page 5). The commands « ifconfig » or « ip link » display the name of all the network card connected in your PC.

Screen display	Comments	Actions to achieve
`Link detected: yes`	Verify that the link is up on this interface.	*watch ethtool enp0s3* *Info : the last line display the link state (Link detected <yes/no>)* Wait until the link is up. Otherwise, plug the cable into the other network card. When the link is detected, stop the command with the *<Ctrl> + c keys*
	Do the same operation with the second card (eth1) and the cable connected to the consultation network.	*watch ethtool xxxxxx* Info : On the consultation network's side, connect a network equipment (Ethernet or PLC switch, WIFI AP, etc) to ensure a permanent network link even if all consultation stations are off.

`[root@localhost ~]# ping -c3 www.google.fr`
`PING www.google.fr (216.58.211.99) 56(84) bytes of data.`
`64 bytes from par03s15-in-f99.1e100.net (216.58.211.99): icmp_s`
`64 bytes from par03s15-in-f99.1e100.net (216.58.211.99): icmp_s`
`64 bytes from par03s15-in-f99.1e100.net (216.58.211.99): icmp_s`
 	
`--- www.google.fr ping statistics ---`
`3 packets transmitted, 3 received, 0% packet loss, time 2003ms`
`rtt min/avg/max/mdev = 28.971/29.768/30.546/0.658 ms`
	Test your Internet connectivity	*ping -c3 www.google.com*

Download the installation file

This file is an archive file named : alcasar-x.y.tar.gz ('x.y' means the version number you want). You can download it in two different ways (USB flash drive or FTP) :

- <u>via an USB flash drive :</u> Download the latest version on the ALCASAR website and copy it on an USB flash drive. Then, use the following procedure to copy it on ALCASAR computer :

Screen display	Comments	Actions to achieve

`[root@localhost ~]# fdisk -l`
 	
`Disque /dev/sda: 80.0 Go, 80032038912 octets`
`255 heads, 63 sectors/track, 9730 cylinders`
`Units = cylindres of 16065 * 512 = 8225280 bytes`
`Disk identifier: 0x75adc3f6`
 	
`Périphérique Amorce   Début      Fin    Blocs   Id  Système`
`/dev/sda1   *         1       1275   10241406   7  HPFS/NTFS`
`/dev/sda2           1276       6630  43014037+  f  W95 Etendu (LBA)`
`/dev/sda5           1276       2550  10241406   7  HPFS/NTFS`
`/dev/sda6           2551       3832  10297633+ 83  Linux`
`/dev/sda7           3833       4081   2000061  82  Linux swap / Solaris`
`/dev/sda8           4082       6630  20474011  83  Linux`
 	
`Disque /dev/sdb: 1031 Mo, 1031798784 octets`
`16 heads, 32 sectors/track, 3936 cylinders`
`Units = cylindres of 512 * 512 = 262144 bytes`
`Disk identifier: 0xcd1d7d24`
 	
`Périphérique Amorce   Début      Fin    Blocs   Id  Système`
`/dev/sdb1   *         1       3936   1007600   e  W95 FAT16 (LBA)`
`[root@localhost ~]#`
	Insert the USB flash drive.
	
	Display informations on mass media storage to get the name of your USB flash drive. In this example, "/dev/sdb1" is a 1GB USB flash drive.
		fdisk -l
		
		Info : You also can display the system log to get this name (journalctrl -f).

`[root@localhost ~]# mkdir /media/usb`
 	
`[root@localhost ~]# mount /dev/sdb1 /media/usb/`
 	
`[root@localhost ~]# cp /media/usb/alcasar-* .`
 	
`[root@localhost ~]# umount /media/usb/`
	• Create a directory and mount the USB flash drive on it.
	• Copy the archive of ALCASAR to the directory "/root".
	• Unmount the USB flash drive.
	• Unplug it.
		mkdir -p /media/usb
		mount /dev/sdb1 /media/usb/
		cp /media/usb/alcasar- /root/*
		umount /media/usb
		
		Info : Replace "sdb1" with the device name retrieved in the previous step.

- <u>via FTP :</u> directly from the ALCASAR computer, download the archive file from the FTP server :

Screen display	Comments	Actions to achieve

`[root@localhost ~]# lftp ftp.alcasar.net/pub`
`cd ok, cwd=/pub`
`lftp ftp.alcasar.net:/pub> cd stable`
`cd ok, cwd=/pub/stable`
`lftp ftp.alcasar.net:/pub/stable> ls`
`-rw-r--r--   1 root     root    87551026 Oct 16 05:35 alcasar-2.8.1.tar.gz`
`-rw-r--r--   1 root     root    87547182 Jan 27  2014 alcasar-2.8.tar.gz`
`lftp ftp.alcasar.net:/pub/stable> get alcasar-2.8.tar.gz`
`87547182 octets transférés en 90 secondes (950.4Ko/s)`
`lftp ftp.alcasar.net:/pub/stable> bye`
`[root@localhost ~]#`
	• Connect to the FTP server with the "lftp" command
	• change to the directory "stable" and list its content
	• download the archive file
	• quit
		lftp ftp.alcasar.net/pub
		cd stable
		ls
		get alcasar-x.y.tar.gz
		bye

Screen display	Comments	Actions to achieve

`[root@localhost ~]# sha256sum alcasar-2.7-test.tar.gz`
`aa6a06936664eb209b8aa7e2160fd0350094c6785de3ae27d1801d29492477ba`
 	
alcasar-v2.7-test
Description courte: SHA256 :
aa6a06936664eb209b8aa7e2160fd0350094c6785de3ae27d1801d29492477ba
Envoyé le: 30 Jan 2013
Téléchargements: 138
Version: 2.7-test
	• Compute the SHA256 digital footprint of this archive and compare it with that of the website.	*sha256sum alcasar-x.y.tar.gz*
		
		Info : If the digital footprint doesn't match, download the archive again. If the problem occurs one more time, ask the developer team via the forum.

`[root@localhost ~]# tar -zxvf alcasar.1-5RC4.tar.gz _`
 	
`[root@localhost ~]# cd alcasar-1.8a`
`[root@localhost alcasar-1.8a]# sh alcasar.sh -i`
	• Uncompress and extract this archive.
	• Move to the directory of ALCASAR and run the installation script.
		tar -xvf alcasar-x.y.tar.gz
		cd alcasar-x.y
		sh alcasar.sh -i

ALCASAR V2.9 Installation Application Libre pour le Contrôle d'Accès Sécurisé et Authentifié au Réseau **** Licence d'utilisation **** ALCASAR est un logiciel libre Avant de l'installer, vous devez accepter les termes de sa licence 'GPL-V3' Le descriptif de cette licence est disponible dans le fichier 'GPL-3.0.txt' Une traduction française est disponible dans le fichier 'GPL-3.0.fr.txt'. Les objectifs de cette licence sont de garantir à l'utilisateur : - La liberté d'exécuter le logiciel, pour n'importe quel usage ; - La liberté d'étudier et d'adapter le logiciel à ses besoins ; - La liberté de redistribuer des copies ; - L'obligation de faire bénéficier à la communauté les versions modifiées. Acceptez-vous les termes de cette licence (O/n)? : _	Acceptation of the license	ALCASAR is a free software (open source) developed under the GPLV3 license.
ALCASAR V2.7 Installation Application Libre pour le Contrôle d'Accès Sécurisé et Authentifié au Réseau Network parameters tests : .... : ok	The network configuration is tested.	
installation de php-ctype-5.1.6-1mdv2007.0.i586.rpm Préparation ... 75/100: php-ctype installation de php-ftp-5.1.6-1.1mdv2007.0.i586.rpm Préparation ... warning: php-ftp-5.1.6-1.1mdv2007.0: Header V3 DSA signature: NOKEY, key ID 2245 8a98 76/100: php-ftp installation de php-gettext-5.1.6-1mdv2007.0.i586.rpm Préparation ...	The installation of about a hundred of software (packages) is done from Internet. Estimated time : 3'	
ALCASAR V2.7 Installation Application Libre pour le Contrôle d'Accès Sécurisé et Authentifié au Réseau Enter the name of your organism :	Enter the name of your organization (without spaces)	Example : rasacla Info : This name is mandatory. The only characters allowed are : [a-z] [A-Z] [0-9] [-]
ALCASAR V2.7 Installation Application Libre pour le Contrôle d'Accès Sécurisé et Authentifié au Réseau The default ALCASAR IP address on consultation network is : 192.168.182.1/24 Do you want to use this IP address and this IP addressing plan (recommanded) (Y/n)? : n Enter ALCASAR IP address in CIDR format (a.b.c.d/xx) : 172.16.0.1/24	Define the IP address of ALCASAR and the network addressing plan of the consultation network. You can accept the default one or change it.	Enter « Y » or « N » Info : If you type "N", the script will ask you for the IP address of ALCASAR and the subnet mask in CIDR notation (ex: 172.16.0.1/16)
ALCASAR V2.7 Installation Application Libre pour le Contrôle d'Accès Sécurisé et Authentifié au Réseau Define the first account allow to administrate the portal : Account : _	Enter the username and password for a first ALCASAR administrative account.	Info : This Linux account is used to administer ALCASAR from the consultation network via the graphical control center (http://alcasar). This is not a consultation user account.
Enf of ALCASAR install process Application Libre pour le Contrôle Authentifié et Sécurisé des Accès au Réseau (ALCASAR) - The system will be rebooted in order to operate ALCASAR - Read the exploitation documentation - The ALCASAR Control Center (ACC) is at http://alcasar Hit 'Enter' to continue	The installation is complete. The system will be restarted to synchronize all components of ALCASAR.	Once the system is restarted, connect an equipment on the consultation network and use it for log in on the portal (http://alcasar). Create the first users. Read the operating instructions carefully ("alcasar-exploitation-en.pdf").

`alcasar-rexy:~# alcasar-daemon.sh`
`17 services are started. All is ok`
`alcasar-rexy:~# _`
	Once the system is restarted, you can check that all needed services are really started. Login on the system and run the command "alcasar-daemon.sh".	If one or more services are not started, the script will attempts to start them.

3. Stop, uninstall, re-install or update ALCASAR

You can stop the ALCASAR computer with the power button, or with the command « *poweroff* » or via the WEB ALCASAR Control Center (ACC).

You can uninstall the portal with the command « *sh alcasar.sh --uninstall* ». This command uninstalls only ALCASAR. The operating system (Linux Mageia) is still present.

If you launch the installation again or if you launch the installation of a newer version on a running version of ALCASAR, the script will ask you if you want to perform an update.

4. Preparation of an off-line installation

This procedure allow you to install ALCASAR in offline mode. This can be useful when you manage to install ALCASAR in a place with a lack of Internet bandwidth. In this case, it's interesting to create an archive file of all the packages (RPMS) needed. This file will be used instead of the Internet downloading. Use the following procedure :

- Creation of the RPM archive file : on a new PC, install "Mageia Linux" as describe in §2.2. Then, retrieve and uncompress the last ALCASAR archive. Go to the scripts directory « *cd alcasar-x.y/scripts/sbin* » and run the script « *./alcasar-rpm-download.sh* ». This script will create the RPM archive file of your PC architecture (32 or 64 bits). Retrieve this archive file on a USB key.
- Offline installation : after installing the system, retrieve the RPM archive file. Uncompress it and go in its directory. Install all the RPM (*urpmi –no-verify-rpm **). Then, follow the installation process describe in chapter §2.3.

5. ALCASAR settings sheet

The file « */root/ALCASAR-passwords.txt* » contains passwords used internally by the different modules of ALCASAR. It contains, more particularly, the password protecting the bootloader (« GRUB »). It can be consulted via the command « *cat /root/ALCASAR-passwords.txt* ». Be careful : when you enter the GRUB password, you keyboard is map like a "qwerty" keyboard.

Organization name :	
Users authentication page	This page is displayed when a browser tries to access a website.

Portal page allowing:
• the administrator to access the control center.
• The users to
   ○ log them out
   ○ change their password
   ○ install the certificate of the Certification Authority (C.A.) in their browsers.
	http://alcasar
	
	Info : The possibilities of the ALCASAR Control Center (ACC) are described in the "ALCASAR-exploitation" document.

Linux accounts	root password : .... sysadmin password : ....
First ALCASAR WEB administrative account	Login: .... password : …...................
Network parameters • IP address of the ISP's equipment (router) : • IP address of DNS servers : • IP address of ALCASAR (WAN/Internet side) : • IP address of ALCASAR (LAN side) :	• ____.____.____.____ • DNS1 :____.____.____.____ • DNS2 :____.____.____.____ • ____.____.____.____/___ • ____.____.____.____/___