



## EXPLOITATION

This document describes how to exploit and administer ALCASAR with the graphical ALCASAR Control Center (ACC) or by using Linux command lines.

Project : ALCASAR	Author : Rexy and 3abtux with support of « ALCASAR Team ». Thanks to translators.
Object : Exploitation	Version : 2.8
Keywords : captive portal, access control, accountability, traceability, authentication	Date : 2013 December

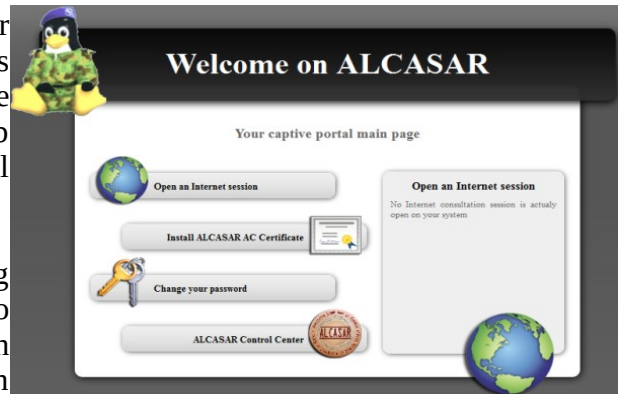
# Table of contents

1. <a href="#">Introduction</a> .....	3
2. <a href="#">Network configuration</a> .....	4
2.1. ALCASAR parameters.....	5
2.2. Consultation equipment parameters.....	5
3. <a href="#">Managing equipment</a> .....	7
4. <a href="#">Managing users</a> .....	7
4.1. Creating a user group.....	7
4.2. Editing and removing a group.....	8
4.3. Creating a user.....	9
4.4. Searching and editing a user.....	10
4.5. Importing users.....	11
4.6. Emptying the users database.....	11
4.7. Authentication exceptions.....	11
5. <a href="#">Filtering</a> .....	12
5.1. Filtering domain names, URLs and the results of search engines.....	12
5.2. Filtering network flows.....	13
5.3. Filtering exceptions.....	14
6. <a href="#">Access to Statistics</a> .....	14
6.1. Number of connections per user per day.....	14
6.2. Connection status of users.....	14
6.3. Daily use.....	15
6.4. Network statistics.....	16
6.5. Security Report.....	17
7. <a href="#">Backup</a> .....	17
7.1. Of the connection traces.....	17
7.2. Of the users database.....	17
7.3. Of the configuration files.....	17
8. <a href="#">Advanced features</a> .....	18
8.1. Administration accounts management.....	18
8.2. Secure administration through Internet.....	18
8.3. How to display the logo of the organization.....	20
8.4. Use of the server certificate.....	21
8.5. Use of an external directory server (LDAP or AD).....	22
8.6. Integration in a complex architecture (AD, external DHCP, LDAP).....	23
8.7. Encryption of log files.....	24
8.8. Managing multiple Internet connections (load balancing).....	25
8.9. Creating a dedicated housing (appliance) ALCASAR.....	25
8.10. Portal by-pass.....	25
9. <a href="#">Shutdown, updates and reinstallation</a> .....	26
9.1. Shutdown.....	26
9.2. Updates of the operating system.....	26
9.3. ALCASAR updates.....	26
9.4. Reinstallation of a portal.....	26
10. <a href="#">Troubleshooting</a> .....	27
10.1. Network connectivity.....	27
10.2. Available disk space.....	27
10.3. Server services.....	27
10.4. Connectivity of the clients.....	27
10.5. Connection to ALCASAR with a serial terminal.....	28
10.6. Troubleshooting.....	29
11. <a href="#">Security</a> .....	30
11.1. On ALCASAR.....	30
11.2. On the consultation network.....	30
12. <a href="#">Annexes</a> .....	32
12.1. Useful commands and files.....	32
12.2. Authentication exceptions helpful.....	33
12.3. Sheet of User.....	34

# 1. Introduction

ALCASAR is an authenticated and secure captive portal. This paper describes how to exploit and administer it with the Alcasar Control Center (ACC) or by using Linux command lines.

The portal welcome page is available for any WEB browser connected on the consultation network. The URL is <http://alcasar>. It allows users to connect, to disconnect, to change their password and to load the security certificate into their web browsers. It allows administrators to access to the graphical ALCASAR Control Center (A.C.C.).



For users connected on the consultation network, the following interception page is displayed when their WEB browser tries to join an Internet WEB site. This interception page is displayed in one of 6 languages (English, Spanish, German, Dutch, French and Portuguese) depending of browsers preferences. Until the user doesn't succeed the authentication process, no network frames from their equipment can pass through ALCASAR.

## Network Access Control

### Information System Security

- That control was set up regulations to ensure traceability, accountability and non-regulation of connections.
- The recorded data can be able to be operated by a judicial authority in the course of an investigation.
- Your activity on the network is registered in accordance with privacy.
- These data will be automatically deleted after one year.
- Click [here](#) to change your password or to integrate the security certificate in your browser.



## Contrôle d'accès au réseau

### Sécurité des Systèmes d'Information

- Ce contrôle a été mis en place pour assurer réglementairement la traçabilité, l'imputabilité et la non-répudiation des connexions.
- Les données enregistrées ne pourront être exploitées que par une autorité judiciaire dans le cadre d'une enquête.
- Votre activité sur le réseau est enregistrée conformément au respect de la vie privée.
- Ces données seront automatiquement supprimées au bout d'un an.
- Cliquez [ici](#) pour changer votre mot de passe ou pour intégrer le certificat de sécurité à votre navigateur.



For administrators, ACC is available in a cipher way (https) in two languages (English and French). After succeeding in the authentication process, the ACC is displayed in one of the three following profiles (cf. §7.1) :

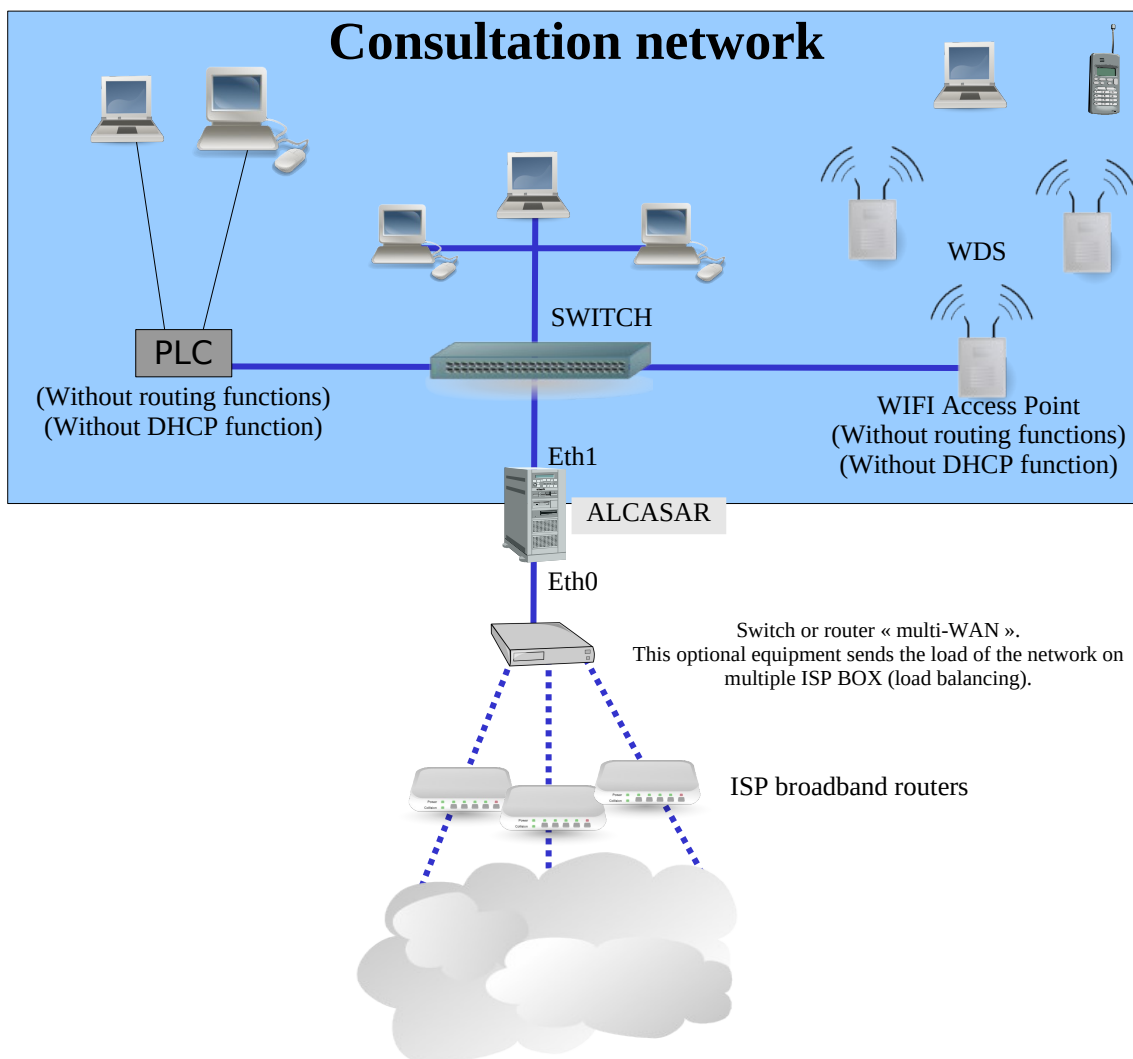
- profile « admin » can use all the administration functions ;
- profile « manager » limited to the users management functions ;
- profile « backup » limited to backup log files functions.

Type	Percent Capacity	Free	Used	Size
Physical Memory	80%	59.31 MB	436.73 MB	495.04 MB
- Kernel + applications	57%		282.22 MB	
- Buffers	5%		26.23 MB	
- Cached	26%		128.28 MB	
Disk Swap	0%	822.07 MB	0.00 KB	822.07 MB

Mount	Type	Partition	Percent Capacity	Free	Used	Size
/	ext4	/dev/sda1	50%	880.09 MB	980.48 MB	1.91 GB
/tmp	ext4	/dev/sda6	2%	1.78 GB	34.97 MB	1.91 GB
/home	ext4	/dev/sda7	2%	1.88 GB	34.95 MB	1.91 GB
/var	ext4	/dev/sda8	12%	1.11 GB	158.09 MB	1.33 GB

**Warning:** The intrusion detection system of ALCASAR will forbid new connection attempts during 3' if it detects three connection failures on ACC.

## 2. Network configuration



On the consultation network, the equipment can be connected with multiple technologies (wired Ethernet, WiFi, PCL, etc.). This network is connected to the ALCASAR Ethernet card « eth1 ». For all these equipment, ALCASAR is the DNS, the time server and the default gateway.

**Warning :** On the consultation network, no other gateway should be present (verify the PLC and WIFI configurations).

The IP address configuration of the consultation network is defined during the installation process of the portal.

### Example of a class C consultation network (default configuration)

- Network IP Address : 192.168.182.0/24 (sub-net mask : 255.255.255.0) ;
- Max number of equipments : 253 ;
- ALCASAR eth1 IP address : 192.168.182.1/24 ;
- Parameters of connected equipments :
  - available IP addresses : between 192.168.182.3 and 192.168.182.254 (statics or dynamics) ;
  - DNS server address : 192.168.182.1 (ALCASAR IP address) ;
  - DNS suffix : localdomain (this DNS suffix must be set in the configuration of static address equipments) ;
  - Default gateway IP address : 192.168.182.1 (ALCASAR IP address) ;
  - network mask : 255.255.255.0

## 2.1. ALCASAR parameters

In the « system » + « network » menu you can see ALCASAR network parameters.

### a) IP configuration

The screenshot shows the 'Network configuration' window. It is divided into three main sections:

- INTERNET** (with a green checkmark):
  - Public IP address : [redacted]
  - DNS1 : [redacted]
  - DNS2 : [redacted]
- Eth0 (Internet connected interface)**:
  - IP Address : 192.168.0.1/24
  - Gateway : 192.168.0.254
- Eth1 (Private network)**:
  - IP Address : 192.168.182.1/24

Currently, these parameters cannot be modified directly with the ACC. Nevertheless, you can change them in a text console by editing the file « `/usr/local/etc/alcasar.conf` ». Once modifications have been made, activate them with the command line « `alcasar-conf.sh --apply` ».

### b) DHCP server

The DHCP (Dynamic Host Control Protocol) server provides dynamically the network parameters to the equipments connected on the consultation network. You can choose one of the three following mode for this server.

The screenshot shows the 'DHCP service' configuration window. It includes:

- Current mode : Full DHCP** (with a dropdown menu showing Full DHCP, No DHCP, Half DHCP, and Full DHCP selected).
- Apply changes** button.
- The different modes are the following :**
  - No DHCP : The DHCP server is off.
  - Half DHCP : The first half of LAN's equipments are in static mode, the other are in dynamic mode (DHCP).
  - Full DHCP : The DHCP server manage all equipments in DHCP mode. Some static addresses can be reserved (see below).
- Static IP addresses reservation** section with a table:

MAC Address	IP Address
exemple : 12-2f-36-a4-df-43	exemple : 192.168.182.10

When this service is on :

- you can reserve IP addresses for equipment that need static IP addresses (servers, printers, WIFI Access Point) ;
- be sure that no other DHCP server is connected on your network. Or be sure to well knowing how manage multi-DHCP service (cf. §8.5a to manage the cohabitation with a A.D. © server).

## 2.2. Consultation equipment parameters

An explanation sheet for users is available at the end of this paper.

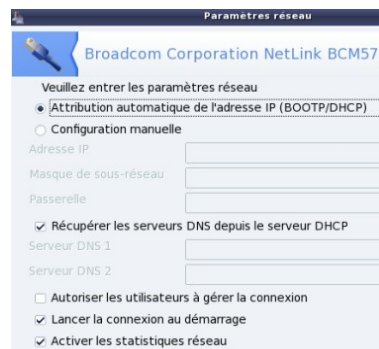
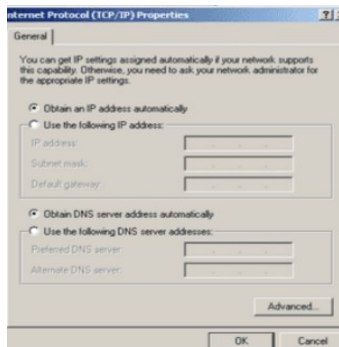
The users only need a simple WEB browser accepting « JavaScript » and « pop-up » windows. To be intercepted by ALCASAR, the web browser must try to access a **HTTP only** Internet WEB site (default start page). **The proxy parameters must no be activated.**

### a) Network configuration

#### Dynamic address configuration (private user equipment) :

« Windows Seven »

« Mandriva &

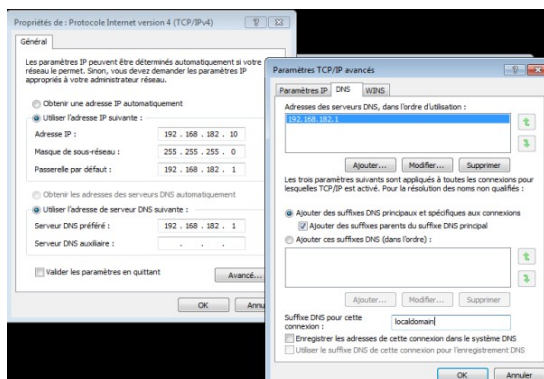


Mageia Linux »

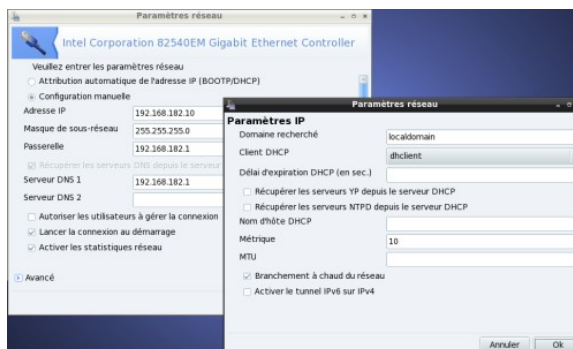
## Static address configuration (servers, printers, WIFI access points, etc.) :

For these equipment, the parameters must be :

- default gateway : IP address of the eth1 card of ALCASAR ;
- DNS server : IP address of the eth1 card of ALCASAR ;
- DNS suffix : localdomain



**« Windows Seven »**



**« Mandriva & Mageia Linux »**

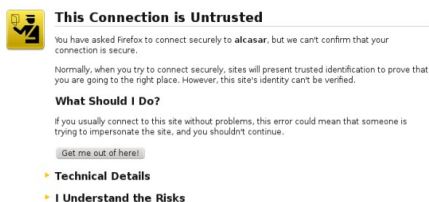
For these static address equipment, be sure to set the DNS suffix to « localdomain ».

### **b) Add bookmark**

On the Web browsers, it can be useful to add a bookmark to the ALCASAR home page (<http://alcasar>) in order to allow users to change their password, to disconnect or to integrate the security certificate into their WEB browsers (cf. : following §).

### **c) How to install the ALCASAR security certificate**

Some communications between consultation equipment and ALCASAR are encrypted with SSL (Secure Socket Layer) protocol. This protocol need two certificates created during the installation process : the ALCASAR certificate and the Local Certification Authority (C.A.) certificate. By default, the WEB browsers don't know this certification authority. So they display the following alert windows when they initially connect to the portal.



**« Mozilla-Firefox »**

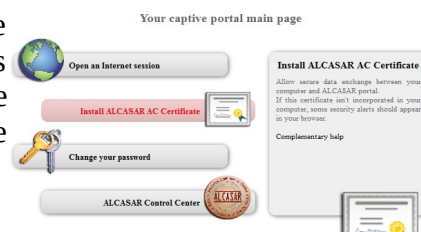


**« Microsoft-I.E. »**



**« Google-chrome »**

Although it is possible to surf, it's interesting to install the security certificate of this C.A. in browsers so that they don't display these alert windows anymore<sup>1</sup>. To do that, click the zone « Install the root certificate » of the portal main page (« <http://alcasar> »). For each web browser, follow the following procedure :

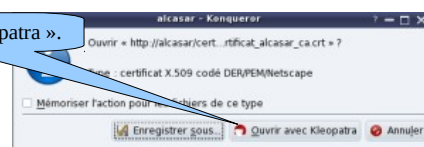


Select « Trust this CA to identify websites ».



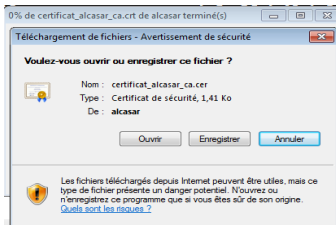
**« Mozilla-Firefox »**

Select : « Open in Kleopatra ».

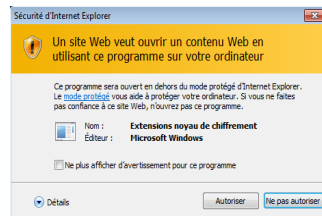


**Konqueror**

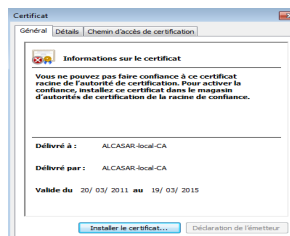
<sup>1</sup> You can avoid this manipulation either in buying and including in ALCASAR an official certificate which is known by all web browsers (see §8.4), or in disabling the encryption of authenticating flow via the script « `alcasar-https.sh {--on|--off}` ». Disabling the encryption of authentication flow implies you totally master your consultation network (see §11).



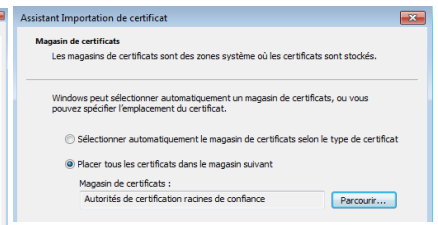
1 – click « open »



2 – click « authorize »



3 – click « install the certificate »



4 – choisissez le magasin « autorité de certification racine de confiance »

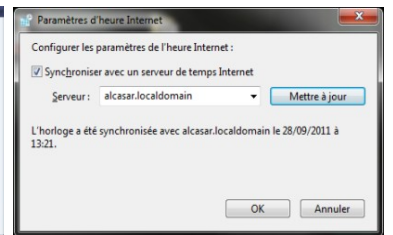
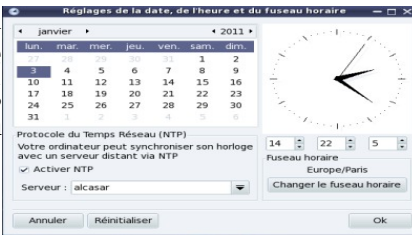
### « Internet Explorer 8 » et « Safari »

« **Google chrome** »: Google Chrome saves the certificate locally (« *certificat\_alcasar\_ca.crt* »). Select « preferences » in the configuration menu, then « advanced options », then « manage certificates » and then « import » in the tab « Authorities ».

### d) Time synchronization

ALCASAR includes a network time server (« NTP » protocol) allowing you to synchronize equipment connected on the consultation network. Thus, on Windows or on Linux, you can define ALCASAR as the time server by right clicking on the clock of the desktop. Write « alcasar » on Linux and « alcasar.localdomain » on Windows.

**Note**: since V2.4, all the Internet NTP flows from consultation equipment are intercepted and redirected to ALCASAR.



## 3. Managing equipment

You can see the list of equipment connected on the consultation network the via the ACC (menu « system » + « activity »).

Activité sur le réseau de consultation				
Cette page est rafraichie toutes les 30 secondes				
#	Adresse IP	Adresse MAC	Usager	Action
1	192.168.182.100	00-21-97-6B-57-E5	██████████	Déconnecter
2	192.168.182.173	00-02-72-85-75-ED	██████████	Déconnecter
3	192.168.182.130	00-16-EA-58-9B-04	██████████	Déconnecter
4	192.168.182.131	00-16-6F-A1-EB-60	██████████	Déconnecter
5	192.168.182.137	00-1A-A0-2F-10-DB	@MAC autorisée	Déconnecter
6	192.168.182.162	00-24-01-0B-95-CB		Dissocier
7	192.168.182.132	00-24-2B-71-24-1C		Dissocier
8	192.168.182.165	00-0F-3D-67-E2-48		Dissocier

Equipment which a user is connected on. You can disconnect him. You can also click on his name to view his parameters

Equipment allowed to pass through ALCASAR without authentication (trusted equipment - see §4.7.c)

Equipment of consultation network without authenticated user. You can remove it (disassociate). This is compulsory when you change the IP address of a static IP equipment or when an equipment is connected with a bad IP address.

## 4. Managing users

You can manage users via ACC after a successful authentication (menu « AUTHENTICATION »). You can :



- create, search, modify and remove users or group of users ;
- create a quick ticket (voucher). Only main attributes are shown and are already configured (example : the expiration date is fixed to the day after) ;
- import user names via a text file or via an users database backup file ;
- empty the users database ;
- define trusted equipment allowed to connect to Internet without authentication (exceptions).

Generally, in order to minimize the administration load, it's interesting to manage group of users instead of each user. For that, the first thing to do is to define the list of group to create.

### 4.1. Creating a user group

When you create a group of users, you can define the attributes of all the users of this group. These attributes are enabled only if they are not empty. Thus, let the attribute empty, if you don't want to use it. Click the

attribute name to see a help popup.

**Create a group**

Already created group(s): test

Group name

Members of group : (separate by a 'space' or a 'carriage return')

Expiration date :=

Authorized period after the first connection (in seconds) :=

Maximum time for a session (in seconds) = S

Maximum time of connection per day (in seconds) := S

Maximum time of connection per month (in seconds) := S

Number of concurrent login :=

Weekly period :=

Maximum of data uploaded (in octets) =

Maximum of data downloaded (in octets) =

Maximum of data exchanged (in octets) =

Maximum upload bandwidth (in kbits/second) =

Maximum download bandwidth (in kbits/second) =

Redirection URL =

**Expiration date**  
After this date, members of this group will not be able to log in anymore. A week after this date, the users will be automatically deleted\*. Click on the zone to see a calendar.

**Authorized period**  
This period begin at the first connection of the user. You can use the drop-down menu to convert days/hours/minutes in seconds.

**3 Limits of time**  
When one of these limits is reached, the user is disconnected. You can use the drop-down menu to convert days/hours/minutes in seconds.

**Number of concurrent login**  
Examples : 1 = only one session at a time, « empty » = no limit, X = X authorized simultaneous sessions, 0 = account locked.  
Note : It's a good way to temporally lock or unlock a user account

**Authorized periods in a week**  
Example for a period from Monday at 7pm to Friday at 18am : Mo-Fr0700-1800

**5 quality of service parameters (QOS)**  
You can define some limits of use. The volume limits are defined for one session. When the limit value is reached, the user is disconnected.

**URL redirection**  
Once authenticated, the user is redirect to this URL. The URL must include the protocol name. Example : « http://www.site.org »

**Page d'aide : session simultanée**

Cet attribut définit le nombre maximum de sessions simultanées qu'un usager peut ouvrir (non renseigné = infini)  
This attribute defines the maximum number of concurrent logins for a user. It is independent from the number of ports the user is allowed to open in a multilink session.

Close Window

Click the attribute name to see a help popup

\* **Remark** : When a user is deleted from the database, his connection logs are kept in order to be able to impute his connections.

## 4.2. Editing and removing a group

Click the group name to edit its specifications

#	groupe	Nombre d'usagers
1		13
2		2
3		4
4		7
5		7
6		11
7		164
8		186
9		136
10		149
11		158

**Group : classroom1 (-)**

Remove all members of this group :

Are you sure to remove classroom1 ?

**Groups management**

**MEMBERS** **ATTRIBUTES** **REMOVE**

Group : classroom1

Members to remove : classroom1  
lulu paulo sophie

The selected members will be remove from the group.  
Use 'shift' or 'Ctrl' for multiple selection.

Members to add :  
Separate the members with a 'space' or a 'carriage return'

Change

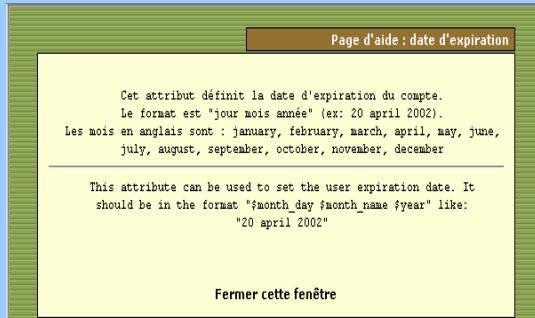
Manage the selected user



### 4.3. Creating a user

Case sensitive for the login and the password (« Dupont » and « dupont » are two different users)

Group membership. In that case, the user inherits of the group attributes\*.



Click the attribute name to see a help popup

Login	<input type="text"/>
Password	<input type="password"/> <input type="button" value="generate"/>
Group	<input type="text"/>
Surname and name	<input type="text"/>
Email Address	<input type="text"/>
Expiration date	:= <input type="text"/>
Maximum time of connection (in seconds)	:= <input type="text"/> S <input type="text"/>
Maximum time for a session (in seconds)	:= <input type="text"/> S <input type="text"/>
Maximum time of connection per day (in seconds)	:= <input type="text"/> S <input type="text"/>
Maximum time of connection per month (in seconds)	:= <input type="text"/> S <input type="text"/>
Number of concurrent login	:= <input type="text"/>
Weekly	<input type="text"/>
Maximum of data upload (in octets)	:= <input type="text"/>
Maximum of data download (in octets)	:= <input type="text"/>
Maximum of data exchanged (in octets)	:= <input type="text"/>
Maximum upload bandwidth (in kbits/second)	:= <input type="text"/>
Maximum download bandwidth (in kbits/second)	:= <input type="text"/>
Redirection URL	:= <input type="text"/>
Voucher language	Portugês <input type="text"/>

see the previous chapter in order to know these attributes

- \* When an attribute is defined both for the user and for its group (example : maximum time for a session), only the user attribute is taken into account.
- \* When a user is member of several groups, the choice of the main group is performed in the user attribute window (see next §).
- \* When a user is locked by one of its attributes, he is warned with a message in the authenticating window (see « user sheet » at the end of this document).

When the user is created, a PDF ticket is generated in the language of your choice.



**i Remark:** if an expiration date is enabled, the user is automatically removed one week after. When a user is deleted from the database, his connections logs are kept in order to be able to impute his connections.

The menu “Create a user” and “Create a quick ticket” allow you to create a page containing 6 tickets. The user's name and user's password are randomly generated. The user's attributes are those written in the form.



## 4.4. Searching and editing a user

You can search a user with several criteria (login name, attribute, etc.). If you let the criteria field empty, all users will be listed.

Search filter

Search criteria: Login

Value (empty = all)

Start search

Search filter

Search criteria: Special attribute

Attribute: Expiration date

Value (empty = all)

Start search

- Expiration date
- Maximum time of connection(in seconds)
- Maximum time for a session(in seconds)
- Maximum time of connection per day(in seconds)
- Maximum time of connection per month(in seconds)
- Number of concurrent login
- Weekly period
- Maximum of data uploaded(in octets)
- Maximum of data downloaded(in octets)
- Maximum of data exchanged(in octets)
- Maximum upload bandwidth(in kbits/second)
- Maximum download bandwidth(in kbits/second)
- Redirection URL

The result is list of users matching your search criteria. The toolbar linked to each user includes the following functions :

User attributes

Préférences du dupont (DUPONT Loïc)

Mot de passe (modification uniquement)

Le mot de passe existe

Durée limite d'une session (en secondes)  3600

Durée limite journalière (en secondes)  10800

Durée limite mensuelle (en secondes)

Période hebdomadaire  wk0800-1700

Date d'expiration  20 june 2009

Membre de  clrisi paul

Change

Personal information

Page d'information personnelle de dupont (DUPONT Loïc)

Nom complet (NOM Prénom) DUPONT Loïc

Mail dupont@loic.fr

Service comptabilité

Téléphone personnel

Téléphone bureau 22020

Téléphone mobile

Modifier

Removal

Suppression du User palette

Êtes-vous certain de vouloir supprimer le user palette ?

Oui supprimer

General information (connections list, statistics, password test, etc.)

Etat des connexions pour paulo (-)

L'utilisateur est en ligne depuis 2009-01-06 22:58:30

Durée des connexions 00:01:26

Serveur alcasar-rexy (192.168.182.1)

Port du serveur 1

@MAC de la station cliente 08-00-27-E7-EA-89

Upload not available

Download not available

Sessions autorisées L'utilisateur peut s'identifier pendant **unlimited time**

Description complète de l'utilisateur -

Check Password

Password

Analyse

	mensuel	hebdomadaire	journalier	par session
limite	none	none	none	none
durée utilisée	0 seconds	0 seconds	00:00:17	



Active sessions (you can disconnect the user)

Fermeture des sessions ouvertes pour l'utilisateur : dupont

L'utilisateur dupont a 1 session(s) ouverte(s)

Êtes-vous certain de vouloir la fermer?

Connections list (you can define an observation period)

Analyse pour rexy

Dates du 2007-12-03 au 2008-05-11

#	logged in	session time	upload	download	server	terminate cause	callerid
1	2007-12-26 14:11:02	17 minutes, 13 seconds	0.65 MBs	7.63 MBs	alcasar-daisi3	User-Request	00-00-56-83-25-0F
2	2007-12-03 15:07:29	10 minutes, 31 seconds	497.71 KBs	2.93 MBs	alcasar-daisi2	User-Request	00-00-56-D9-B1-9B
3	2007-12-03 13:55:50	23 minutes, 20 seconds	1.31 MBs	7.63 MBs	alcasar-daisi2	User-Request	00-00-56-D9-B1-9B
Total pages		51 minutes, 4 seconds	2.41 MBs	18.21 MBs			

Utilisateur: rexy    début date: 2007-12-03    fin date: 2008-05-11    nbr. page: 10    classé le: plus récent en premier  show

## 4.5. Importing users

In the ACC (menu « AUTHENTICATION », « Import ») :

### a) From a backup of users database

When you import a backup of users database, the current database will be emptied. As this running database has to be given in case of investigation, a backup is automatically performed (see §7 to retrieve this backup).

### b) From a text file (.txt)

This function allows you to quickly add users to the current database. This text file must be structured like this : one user login per line followed or not with a password separated with a space. Without a defined password, ALCASAR creates one randomly. This file can come from a spreadsheet application :

- from the « Microsoft office suite », record the file in format « Text (DOS) (\*.txt) » ;
- from the « LibreOffice office suite », record the file in format « Text CSV (.csv) » removing separators (option « edit filter parameters »).

Once the file is imported, ALCASAR creates each new account. If the login name already exists, the password is just changed. Two files in format « .txt » and « .pdf » including login names and passwords are created and saved in the directory « /tmp » (during 24 hours). These files are available in the ACC.

In order to ease the management of new users, you can define their group of ownership. You can define a group which already exist.

For each import job, a file including the login names and the password is shown during 24 hours (format « txt » and « pdf »).

## 4.6. Emptying the users database

This functionality allows you to remove all the users in one click. A backup of this database is automatically performed. See §7 to retrieve the backup. See §4.5.a to re-inject it.

## 4.7. Authentication exceptions

By default, ALCASAR is configured to stop the network flows from equipment without an authenticated user. Nevertheless, you can allow some flows in order to :

- allow antivirus softwares and operating systems to update themselves automatically on the Internet editor sites (See §12.2) ;
- access to a server or to a security zone (DMZ) located behind ALCASAR ;
- allow some equipment not to be intercepted ;
- on Seven©, allow recording the license on the Microsoft site and keep the icon “Internet access” on.

### a) Allow network flows to trusted sites or trusted domain names

In this window, you input trusted site names or trusted domain names. In case of a domain name, all the linked sites are allowed (example : « .free.fr » allows “ftp.free.fr”, “www.free.fr”, etc.). You can display the link of a trusted site on the ALCASAR interception page. The network protocols filtering, if enabled (see § 5.2.c), is applied on these trusted sites or trusted domain names.

Domain names	Link displayed in intercept page	Remove from list	Domain names	Link displayed in intercept page
free.fr		<input type="checkbox"/>	exemple1 :	exemple1 : mydomain
www.alcasar.net	alcasar website	<input type="checkbox"/>	exemple2 : .yourdomain.net	Let empty to not display link
www.wikipedia.org	wikipedia	<input type="checkbox"/>		

### b) Allow network flows to trusted IP addresses or trusted network IP addresses

Trusted IP addresses		
Manage systems addresses or networks IP addresses that can be joined without authentication		
Trusted IP addresses	Comments	Remove from list
192.168.182.3	my_nas	<input type="checkbox"/>
<input type="button" value="Apply changes"/>		
Trusted IP addresses		Comments
exemple1 : 170.25.23.10		my_web_server
exemple2 : 15.20.20.0/16		my_dmz
<input type="text"/>		<input type="text"/>
		<input type="button" value="Add to list"/>

In this window, you manage trusted IP addresses or trusted network ip addresses (a DMZ for example). The network protocol filtering, if enabled (see § 5.2.c), has no effect on the addresses reported here.

### c) Allow trusted consultation equipment



It is possible to allow some equipment to cross ALCASAR consultation without being authenticated. To do this, simply create a standard user whose login name is the MAC address of the equipment (example: 08-00-27-F3-DF-68) and the password is "password". You can enjoy some of the features associated with each user as rate limiting example. It should be borne in mind that in this case, traces of connection to the Internet will be charged to the equipment (not to a user). This operation requires to be approved by the responsible body of SSI.

Once such account created, you must restart the chilli service ("System" + "Services" + "chilli" + "restart") for an immediate activation.

To enhance the display of only the MAC, you can add user information in the "user info" menu (ie: first name).

#	Usager	Actions	Membre du groupe
1	00-11-09-2D-25-4C (PC proviseur)		
2	48-5B-39-4D-0D-77 (PC profs)		
3	fabien_y		elevés
4	jerome_m		elevés
5	laurent_t		elevés

## 5. Filtering

### FILTERING

- ▶ Domain names
- ▶ Network
- ▶ Exceptions

ALCASAR has three optional filters:

- a domain names, URLs and results of search engines filter;
- a network protocols filter;
- an antimalware on the WEB flow.

The first two filters are disabled by default. They were developed at the request of organizations likely to welcome young people (schools, colleges, recreation centers, etc.).

### 5.1. Filtering domain names, URLs and the results of search engines

The filter can be compared to the parental/school control system. It allows you to block access to domain names and URLs referenced in a blacklist. ALCASAR uses a blacklist drawn up by the University of Toulouse. This "blacklist" was chosen because it is distributed under a free license (creative commons) and its content refers to France. In this list, the domain names (eg www.domaine.org) and URL (eg www.domaine.org/rubrique1/page2.html) are classified by categories (games, astrology, violence, sects, etc.). The management interface allows you :

- to update this list and define the categories of sites to block;
- to rehabilitate a blocked site (eg a site that was banned was closed and purchased);
- to add sites or URLs that are not known to the blacklist (CERT alerts, local regulations, etc.).

#### a) Enabling and disabling filtering

Domain names and URL filtering
Actually, the Domain name and URL filter is on
<input type="button" value="Switch the Filter off"/>

#### b) Updating the blacklist

Updating the blacklist will download the latest version of the University of Toulouse blacklist and integrate it to ALCASAR. Once the file is downloaded, ALCASAR calculates and displays its fingerprint. You can then compare this fingerprint with the one available on the website of Toulouse. If the two are identical, you can confirm the update. Otherwise, discard it.

List version : January 05 2013
<input type="button" value="Download the last version"/> (Estimated time : one minute.)
List version : January 05 2013
The digital fingerprint of the downloaded blacklist is : 8498704cd817e4c40f29888a96a18371
Verify it with this link (lme "blacklists.tar.gz") : <a href="https://dsi.ut-capitole.fr/blacklists/download/MD5SUMLIST">dsi.ut-capitole.fr/blacklists/download/MD5SUMLIST</a>
<input type="button" value="Activate the new version"/> (Estimated time : one minute.)
<input type="button" value="Reject"/>

#### c) Modifying the blacklist

You can choose categories to filter. You can restore or add sites to the « blacklist ».

**BlackList**

Select the categories to filter

anel	astrology	audio-video	blog	celebrity	chat	cooking	filehosting	financial	forums
games	lingerie	manga	mobile-phone	publicite	radio	unaffected	shopping	social_networks	sports
webmail	adult	agresstf	dangerous_material	dating	drogue	gambling	hacking	malware	marketingware
mixed_adult	ossi	phishing	redirector	remote-control	sect	strict_redirector	strong_redirector	tricheur	warez

Domain names or URLs rehabilitated

Rehabilitated domain names

Enter here domain names that are blocked by the blacklist and you want to rehabilitate.  
Enter one domain name per row (example : .domain.org)

Rehabilitated URL

Enter here URL that are blocked by the blacklist and you want to rehabilitate.  
Enter one URL per row (example : www.domaine.org/perso/index.htm)

Domain names or URLs to add to blacklist

Filtered domain names

Enter one domain name per row (exemple : .domain.org)

Filtered URL

Enter one URL per row (exemple : www.domaine.org/perso/index.htm)

Save changes (Once validated, 30 seconds is necessary to compute your modifications)

**adult**

Sites related to eroticism and pornography

Number of filtered domain names : 972185  
Number of filtered URL : 49718

By clicking on the category name, you display its definition and the number of domain names and URLs it contains.

**Features:** The "ossi" corresponds to domain names and URLs that you add to the blacklist.

**Info:** if you test screening and rehabilitation, consider clearing the cache browsers.

## d) Special filtering

Two special filters are available in this menu. The first one blocks URLs containing an IP address instead of a domain name. The second one allows you to exclude the results of search engines that may not be suitable for minors (function "safesearch"). This second filter is compatible with "Google", "Yahoo", "bing" and "metacrawler". This filter transforms the Google "https" requests into "http" requests.

**Specific filtering**

Filtering URLs that contain an IP address instead of a domain name (ie: http://25.56.58.59/index.htm)

Enabling school/parental control for the search engines google, yahoo, bing, metacrawler and Youtube.  
For Youtube, enter your ID here :  ([link to create a Youtube ID](#))

Save changes

This filter can work with "YouTube" only if you get a Youtube ID. For that, visit : [http://www.youtube.com/education\\_signup](http://www.youtube.com/education_signup). Once your YouTube account is created, copy your YouTube ID in the ALCASAR Control Center and save the changes.

Option A : ajouter une nouvelle règle d'en-tête HTTP

Modifiez votre filtre de matériel ou vos paramètres de serveur proxy pour que tout le trafic sortant vers youtube.com contienne l'en-tête HTTP personnalisé suivant. L'ID à utiliser dans la configuration de l'en-tête HTTP, écrit ci-dessous, est propre au réseau de votre établissement scolaire. Si votre établissement est bloqué au niveau du quartier, cet en-tête HTTP sera propre au réseau du quartier.

X-YouTube-Edu-Filter:K[redacted]Tm6g

After creating your "Youtube" account, retrieve the « Youtube-EDU-filter » (string characters located after the ':').

## 5.2. Filtering network flows

ALCASAR includes a filter module to allow only network flows deemed necessary.

### a) Antimalware flow WEB

ALCASAR uses the open source software "clamav" to analyze and filter the flow of web pages within the network consultation. It is enabled by default and filters out viruses and spyware (keyloggers, adware). The malwares database is updated every two hours. You can test its operation by downloading a test file located at the URL: [http://eicar.org/anti\\_virus\\_test\\_file.htm](http://eicar.org/anti_virus_test_file.htm)

**WEB antivirus**

Actually, the WEB antivirus is on

Switch the antivirus off

### b) IP addresses or network addresses filtering

This menu allows you to block the access to certain IP addresses (or network IP addresses). A network IP address is preconfigured. It corresponds to the local network between ALCASAR and the Internet router.

**IP address filter**

List of blocked IP addresses (or network IP addresses)

IP addresses	Comments	Blocked	Remove from list
125.45.45.25	CERT-alert	<input type="checkbox"/>	<input type="checkbox"/>
192.168.182.0/24	LAN-ALCASAR-BOX	<input type="checkbox"/>	<input type="checkbox"/>

Save changes

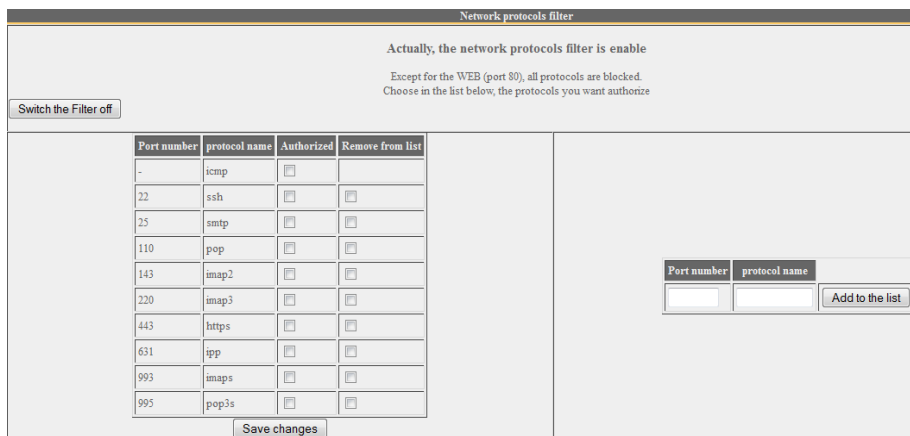
IP address (or network IP address)	Comments
exemple1 : 15.25.26.27	exemple1 : CERT alert
exemple2 : 18.20.20.0/24	exemple2 : LAN of zombies

Add to the list

### c) Protocols filtering

When this filter is not enabled, a user authenticated by the portal can exploit all imaginable protocols (Internet access is limitless). All the actions of authenticated users are traced and recorded regardless of the protocol used.

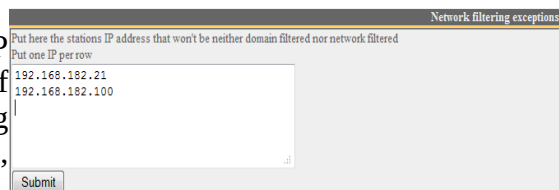
When the filter module is enabled, only the HTTP protocol is enabled by default. All other protocols are blocked. It is possible from this restrictive mode, to enable, one by one, the network protocols you want to allow. A list of standard protocols is presented by default. You can enrich it.



- ICMP: to allow for example the command « ping ».
- SSH (Secure SHell): to allow secured remote connections.
- SMTP (Simple Mail Transport Protocol): to allow sending email from a dedicated client (outlook, thunderbird, etc.).
- POP (Post Office Protocol): to allow mail clients dedicated to recover (increase) the email.
- HTTPS (HTTP secure): to allow secured Web surfing.

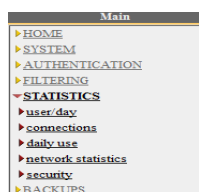
### 5.3. Filtering exceptions

Menu "exception" allow you to define network consultation IP addresses that will not be filtered (domain names, URLs, results of search engines and network protocols). Antimalware filtering remains active. This capability is for management staff, adults, teachers, etc.



## 6. Access to Statistics

The interface statistics are available, after authentication on the portal management page (menu "statistics")



This interface provides access to the following information:

- number of connections per user per day (updated every night at midnight);
- connection status of users (updated in real time);
- daily load of the portal (updated every night at midnight);
- network use statistics (updated every 5 minutes);
- security reports (updated in real time).

### 6.1. Number of connections per user per day

This page displays, per day per user, number, connection time and volumes of data exchanged. Warning: the volume of data exchanged is what ALCASAR sent to the user (upload) and what it received from the user (download).

	User name	Number of connections	Cumulative time	Volume of data exchanged		
67	2007-06-04	chillspot.lyon.fr	3	34 minutes, 58 seconds	1.51 MBs	52.37 MBs
68	2007-06-04	chillspot.lyon.fr	3	17 minutes, 38 seconds	0.78 MBs	3.15 MBs
69	2007-06-04	chillspot.lyon.fr	3	32 minutes, 4 seconds	1.84 MBs	12.61 MBs
70	2007-05-30	chillspot.lyon.fr	4	3 hours, 50 minutes, 26 seconds	3.25 MBs	17.91 MBs
71	2007-06-01	chillspot.lyon.fr	4	57 minutes, 16 seconds	4.04 MBs	23.44 MBs
72	2007-05-31	chillspot.lyon.fr	4	1 hours, 20 minutes, 26 seconds	6.80 MBs	26.79 MBs
73	2007-05-30	chillspot.lyon.fr	4	50 minutes, 32 seconds	4.03 MBs	29.53 MBs
74	2007-05-30	chillspot.lyon.fr	4	32 minutes, 49 seconds	1.79 MBs	11.75 MBs
75	2007-06-05	chillspot.lyon.fr	5	21 minutes, 22 seconds	1.97 MBs	71.12 MBs
76	2007-05-31	chillspot.lyon.fr	5	1 hours, 12 minutes, 26 seconds	0.88 MBs	4.71 MBs
77	2007-06-01	chillspot.lyon.fr	5	1 hours, 3 minutes, 25 seconds	1.41 MBs	59.74 MBs
78	2007-05-30	chillspot.lyon.fr	6	25 minutes, 10 seconds	1.86 MBs	61.05 MBs
79	2007-06-04	chillspot.lyon.fr	6	1 hours, 11 minutes, 4 seconds	6.33 MBs	39.43 MBs
80	2007-06-05	chillspot.lyon.fr	7	33 minutes, 45 seconds	1.40 MBs	9.79 MBs
81	2007-05-31	chillspot.lyon.fr	8	1 hours, 2 seconds	0.83 MBs	32.22 MBs
82	2007-05-30	chillspot.lyon.fr	10	3 hours	17.60 MBs	39.65 MBs
83	2007-05-31	chillspot.lyon.fr	14	3 hours, 51 minutes, 40 seconds	2.63 MBs	15.65 MBs

One line per day

You can customize this state:  
 - Filtering on a particular user;  
 - Defining the period considered;  
 - Sorting with different criteria.

### 6.2. Connection status of users

This page will list the log in and log off events from the portal. An input box allows you to specify your search and display criteria.

Regardless of particular research, the chronological list of connections is displayed (since the installation of the portal). Warning: the volume of data exchanged is what ALCASAR sent to the user (upload) or what it received from the user (download).

Afficher les attributs suivants :

- Accounting Stop Delay
- AcctAuthentic
- CalledStationId
- Caller Id
- Client IP Address

Classé par : Accounting Id

Nbr. Max. de résultats retournés : 40

Envoyer

Set your display criteria here. Criteria have been pre-defined. They meet most needs (user name, IP address, connection start, end connection, volume of exchanged data). Use the <Ctrl> and <Shift> to change the selection.

Set your search criteria here. By default, no criteria is selected. The list of connections made since the installation of the portal will be displayed in chronological order. Two examples of particular research are given below.

- Example of search No1 : Display in chronological order of the connections established between June 1 and June 15, 2009 with the default display criteria:

Client IP Address	Download	Login Time	Logout Time	Session Time	Upload	User Name
192.168.182.10	443.61 KBs	2009-05-29 11:19:54	2009-05-29 11:32:34	12 minutes, 40 seconds	11.52 MBs	
192.168.182.22	1.66 MBs	2009-06-03 18:24:20	2009-06-03 18:44:20	20 minutes	33.55 MBs	
192.168.182.129	46.12 MBs	2009-06-03 18:58:23	2009-06-04 09:39:01	14 hours, 40 minutes, 38 seconds	1.10 GBs	
192.168.182.10	381.81 KBs	2009-06-04 12:58:10	2009-06-04 13:06:08	7 minutes, 58 seconds	1.77 MBs	
192.168.182.10	400.14 KBs	2009-06-04 13:41:29	2009-06-04 13:43:45	2 minutes, 16 seconds	1.55 MBs	
192.168.182.10	327.07 KBs	2009-06-04 14:50:24	2009-06-04 15:22:37	32 minutes, 13 seconds	1.29 MBs	
192.168.182.10	96.93 KBs	2009-06-04 15:23:13	2009-06-04 15:37:46	14 minutes, 33 seconds	443.14 KBs	
192.168.182.10	286.75 KBs	2009-06-04 15:38:37	2009-06-04 16:20:42	42 minutes, 5 seconds	375.28 KBs	
192.168.182.129	10.33 MBs	2009-06-04 16:29:46	2009-06-04 19:15:48	2 hours, 46 minutes, 2 seconds	463.62 MBs	
192.168.182.110	303.42 KBs	2009-06-04 16:57:30	2009-06-04 18:05:17	1 hour, 27 minutes, 38 seconds	5.57 MBs	

- Example of search No2 : Display the 5 shortest connections made during the month of July 2009 on the station whose IP address is "192.168.182.129". The display criteria includes the cause of disconnection and does not take into account the volume of data exchanged:

Client IP Address	Login Time	Logout Time	Session Time	Terminate Cause	User Name
192.168.182.147	2009-07-01 14:07:28	2009-07-01 14:08:30	1 minutes, 2 seconds	User-Request	
192.168.182.147	2009-07-21 10:57:19	2009-07-21 10:58:26	1 minutes, 7 seconds	Admin-Reset	
192.168.182.147	2009-07-01 16:21:43	2009-07-01 16:23:00	1 minutes, 17 seconds	User-Request	
192.168.182.147	2009-07-07 09:50:35	2009-07-07 09:54:02	3 minutes, 27 seconds	User-Request	
192.168.182.147	2009-07-01 17:50:50	2009-07-01 17:54:30	3 minutes, 40 seconds	User-Request	

Afficher les attributs suivants :

- Stop Connect Info
- Terminate Cause
- Unique Id
- Upload
- User Name

Classé par : Session Time

Nbr. Max. de résultats retournés : 5

Envoyer

### 6.3. Daily use

This page allows you to know the daily load of the portal.

De 2009-11-23 à 2009-11-30 usager sur le serveur [all] Go

Thursday, 14 January 2010, 18:26:58 CET

Période observée : 2009-11-23 à 2009-11-30

### Statistiques d'utilisation journalière

Statistiques pour tous les usagers

Champs affichés : Nbre de sessions Temps d'utilisation total uploads

Rafraîchir

date	sessions	temps d'utilisation total	uploads
2009-11-23	266 72%	07:02:12:03 85%	3.72 GBs 32%
2009-11-24	266 72%	05:06:42:09 63%	3.66 GBs 31%
2009-11-25	314 85%	07:00:29:46 84%	5.96 GBs 52%
2009-11-26	305 83%	07:18:28:08 93%	5.73 GBs 50%
2009-11-27	366 100%	08:07:32:27 100%	10.59 GBs 92%
2009-11-28	235 64%	05:02:06:34 61%	11.45 GBs 100%
2009-11-29	253 69%	05:06:26:55 63%	9.85 GBs 86%
2009-11-30	280 76%	07:09:22:28 88%	7.29 GBs 63%

	sessions	temps d'utilisation total	uploads
maximum	366	08:07:32:27	11.45 GBs
moyenne	286	06:15:40:04	7.28 GBs
récapitulatif	2285	53:05:20:30	58.25 GBs

Set here the period. You can specify a particular user (leave this field blank to accommodate all users).

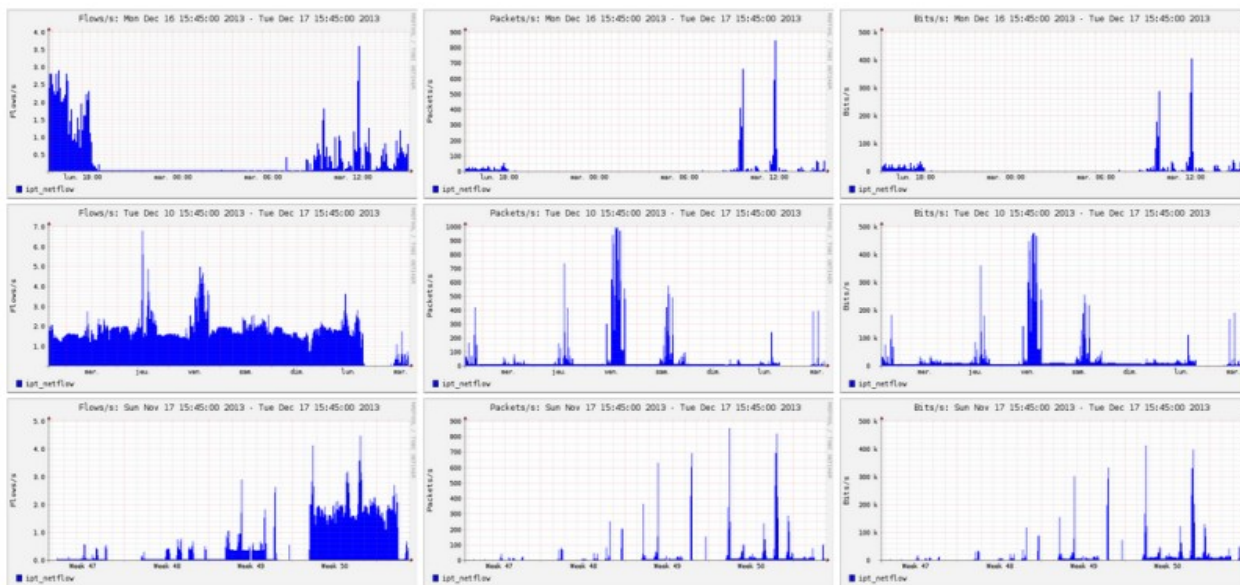
## 6.4. Network statistics



This page shows the statistics about outbound network traffic (by day, by week and by month). The data are update every 5'.

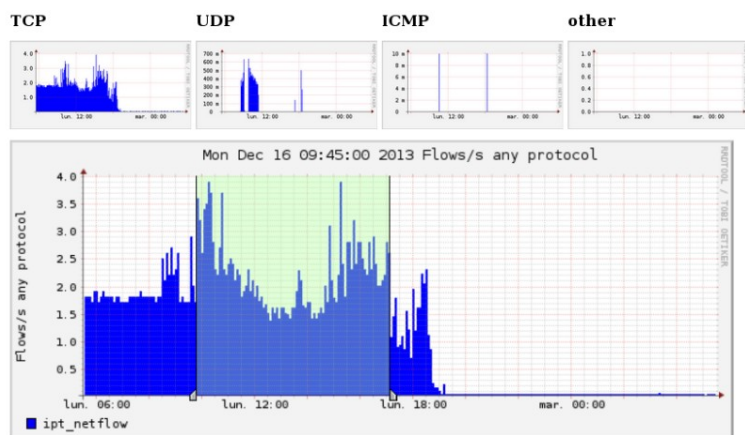
Home | Graphs | Details | Alerts | Stats | Plugins | live | Bookmark URL | Profile: live ▼

### Overview Profile: live, Group: (nogroup)



The “details” menu allows you to zoom on a particular time slot. For the HTTP flows, the network IP addresses are hidden and replaced with the IP address of ALCASAR.

#### Profile: live



#### Netflow Processing

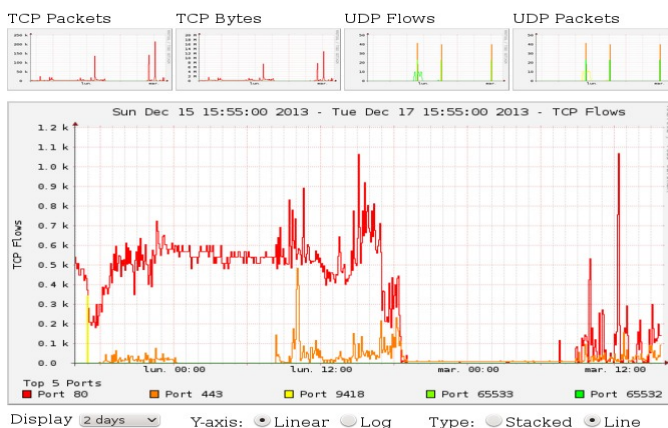
Source: ipt\_netflow | Filter: | Options: List Flows, Stat TopN, Top: 10, Stat: DST Port, order by: bytes, Limit: Packets > 0, Output: / IPv6 long

```

++ nfdump -M /var/log/nfsen/profiles-data/live/ipt_netflow -T -R 2013-12-16/nfcapd.201312160945:2013
nfdump filter:
any
Top 10 Dst Port ordered by bytes:
Date First seen Duration Proto Dst Port Flows(%) Packets(%) Bytes(%)
2013-12-16 09:44:48.692 26689.479 any 80 50589 (86.6) 730755 (98.9) 61.3 M (99.2)
2013-12-16 09:44:54.617 26683.314 any 443 5180 (8.9) 5217 (0.7) 322601 (0.5)
2013-12-16 09:56:00.115 5470.785 any 21592 150 (0.3) 186 (0.0) 12097 (0.0)
2013-12-16 10:04:10.241 4963.755 any 1030 12 (0.0) 106 (0.0) 8351 (0.0)
2013-12-16 09:50:43.605 281.302 any 27019 120 (0.2) 120 (0.0) 5120 (0.0)
2013-12-16 10:39:26.645 19.331 any 60225 1 (0.0) 40 (0.0) 3145 (0.0)
2013-12-16 09:50:42.985 2.051 any 27017 46 (0.1) 46 (0.0) 2944 (0.0)
2013-12-16 09:50:42.985 2.051 any 27018 46 (0.1) 46 (0.0) 2944 (0.0)
2013-12-16 09:45:35.640 22558.334 any 993 43 (0.1) 43 (0.0) 2729 (0.0)
2013-12-16 10:33:58.632 20569.346 any 21 31 (0.1) 33 (0.0) 1980 (0.0)
Summary: total flows: 58436, total bytes: 61.8 M, total packets: 739076, avg bps: 18520, avg pps: 27,
Time window: 2013-12-16 09:44:48 - 2013-12-16 17:09:38
Total flows processed: 58436, Blocks skipped: 0, Bytes read: 3049352
Sys: 0.024s Flows/second: 2337814.1 Wall: 0.020s Flows/second: 2851927.8
    
```

#### PortTracker

#### Port Tracker



The “plugins” menu shows the network traffic by protocols (port tracker). You can see the protocols used “now” or all protocols seen during the last “24 hours”.



## 6.5. Security Report



This page displays three safety information identified by ALCASAR, namely:

- The list of users disconnected due to an attempt of spoofing the MAC address of their equipment;
- The list of malware intercepted by the integrated antivirus;
- The list of IP addresses banned during 5' by the intrusion detection system. The reasons can be : 3 successive failures with SSH – 5 successive connexion failures on ACC – 5 successive connexion failures of users – 5 successive attempts to change password in less than one minute.

The screenshot shows three sections of the Security Report:

- Adresse(s) MAC usurpée(s) (Watchdog):** Lists multiple instances of MAC address spoofing. A callout box points to the text: "User disconnected due to MAC address spoofing".
- Virus bloqué(s) (HAVP):** Lists blocked malware. A callout box points to the text: "Malware blocked EICAR test files, Trojans, Virus".
- Adresse(s) IP bloquée(s) (Fail2Ban):** Lists blocked IP addresses. A callout box points to the text: "IP addresses blocked by IDS".

## 7. Backup

### 7.1. Of the connection traces

The menu "Backup" from the management interface presents in first column, the log files of the consultation equipment. These files include the users database. To archive them on an other media, "right click" on the file name and click "save target as". These files are automatically generated once a week (in the directory « `/var/Save/archive/` » of the portal). The files older than one year are removed.

Traceability log files	
archive-20140103-18h59.tar.gz	(1.82 Mo)
archive-20131216-05h35.tar.gz	(572.83 Ko)
archive-20131209-05h35.tar.gz	(604.04 Ko)
archive-20131202-05h35.tar.gz	(761.29 Ko)
archive-20131125-05h35.tar.gz	(931.33 Ko)
archive-20131118-05h35.tar.gz	(732.16 Ko)
archive-20131111-05h35.tar.gz	(1.36 Mo)
archive-20131104-05h35.tar.gz	(787.9 Ko)
archive-20131028-05h35.tar.gz	(848.86 Ko)
archive-20131021-05h35.tar.gz	(938.89 Ko)
archive-20131014-05h35.tar.gz	(643.25 Ko)
archive-20131007-05h35.tar.gz	(588.05 Ko)

It's possible to generate the log file of the current week. The name of this file is different : "traceability-date-..."

Create the active traceability file

### In case of judicial inquiry

In the context of a judicial investigation, the law enforcement officials may ask you to trace connections of your users. You just have to provide the archive file corresponding to the week covering the date of the offense. If investigators ask files of the current week, just generate the active traceability file.

### 7.2. Of the users database

The menu "Backup" from the management interface presents in the second column the files in "SQL" format of the users database including : the username, the encrypted password, attributes and log-in / log-off sessions on the portal. They are generated in the directory « `/var/Save/base/` » of the portal when you select "save the active users databases".

These files can be used to restore a database (see §4.5.a). They are also used during the reinstallation of a portal (see §9.4).

Users database	
radius-20131216-04h45.sql	(365.28 Ko)
radius-20131209-04h45.sql	(347.22 Ko)
radius-20131202-04h45.sql	(327.67 Ko)
radius-20131125-04h45.sql	(309.69 Ko)
radius-20131118-04h45.sql	(290.98 Ko)
radius-20131111-04h45.sql	(268.58 Ko)

Save the active users database

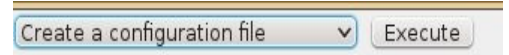
### 7.3. Of the configuration files

In the third column, there are the archive of the configuration files used in case of reinstallation of a portal (due to a hardware failure or hardware

Configuration files	
alcasar-conf-20140103-18h50.tar.gz	(74.04 Ko)
alcasar-conf-20130709-00h23.tar.gz	(117.77 Ko)
alcasar-conf-20130417-22h59.tar.gz	(60.98 Ko)
alcasar-conf-20130406-11h06.tar.gz	(53.61 Ko)
alcasar-conf-20130327-23h11.tar.gz	(46.84 Ko)

change) : see. §9.4.

It's possible to generate a configuration file at any time.



## 8. Advanced features

### 8.1. Administration accounts management

Your ALCASAR server has two system accounts (or Linux accounts) that were created during the installation of the operating system:

- « root » : This is the account used for system administration ;
- « sysadmin » : This account allows you to take secure remote control of yours system (see next §).

Along with these two "system" accounts, "management" accounts have been defined to control some functions through the ACC (ALCASAR Control Center). These "management" accounts can belong to one of the three following profiles:

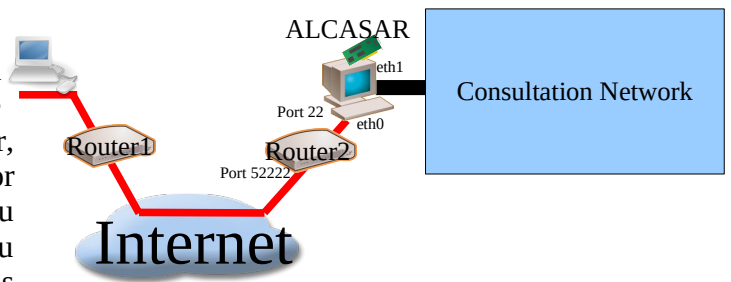
- « **admin** » : this account give access to all the functions of the ACC. A first "admin" account was created during the installation of ALCASAR (see Installation documentation);
- « **manager** » : this account only give access to users and groups management functions (see §4) ;
- « **backup** » : this account only give access to backup and archiving of log files (see §7).

You can create as many management accounts as you want in each profile. To manage these management accounts, use the « `alcasar-profil.sh` » command as « root » :

- `alcasar-profil.sh --list` : to list all the accounts of each profile
- `alcasar-profil.sh --add` : to add an account to a profile
- `alcasar-profil.sh --del` : to delete an account
- `alcasar-profil.sh --pass` : to change the password of an existing account

### 8.2. Secure administration through Internet

It is possible to established a secured remote connection to an ALCASAR portal using encrypted data flow ("SSH protocol" - Secure SHell). Let's take an example of an administrator who seeks to administer, through the Internet, an ALCASAR portal or equipments on the consultation network. Firstly, you need to activate the "SSH" service on ALCASAR (menu "system" and "network"). You must know the IP address of the "Broadband modem/router#2".



#### a) **Broadband modem/router configuration**

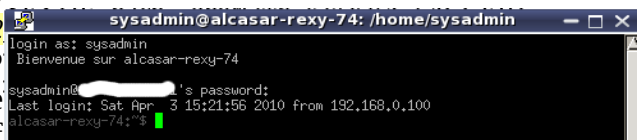
It is necessary to configure broadband modem/router#2 so that it doesn't block the "SSH" protocol. To anonymise the SSH data flow on the Internet, the default port (22) is replaced by another one (52222 for exemple). If you want, you can still use the port 22.

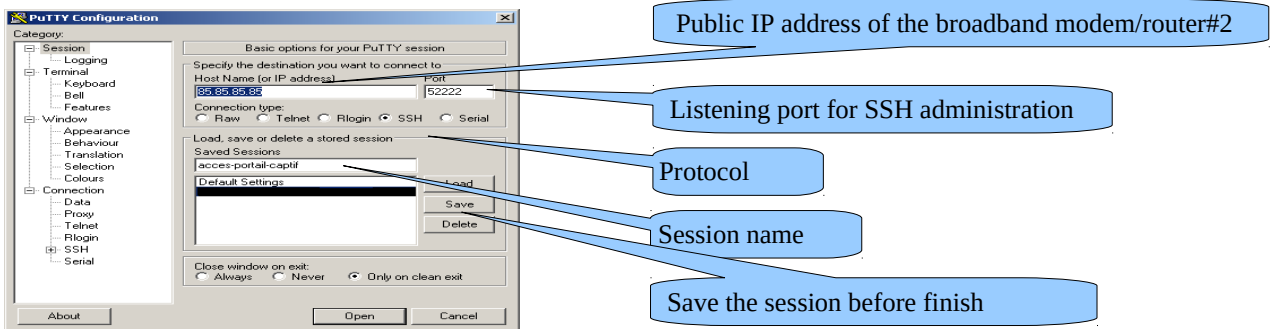
Use the configuration documentation of your broadband modem/router to achieve this.

#### b) **administration of ALCASAR in text mode**

You can log in remotely to ALCASAR using the Linux "sysadmin" account created during the installation of the system. Once you are logged in, you can use the administration commands of ALCASAR (see § 12.1). You can become "root" via the "su" command.

- On Linux, install "openssh-client" (it is also possible to install "putty") and run the command « `ssh -p 52222 sysadmin@w.x.y.z` » (replace « w.x.y.z » by the public IP address of the broadband modem/router#2 and replace the "external\_port" with the listening port number of broadband modem/router#2 (52222 in our example). You can add the "-C" option to activate the compression algorithme.
- On Windows, install "Putty" or "putty-portable" or "kitty" and create a new session:





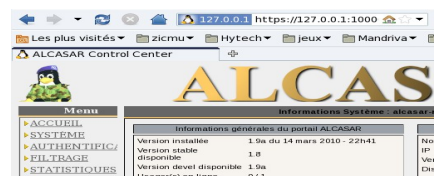
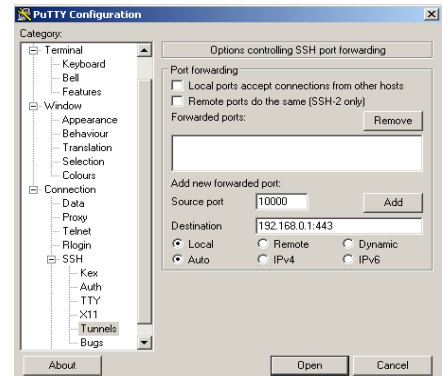
click on "Open", accept the server key and log in as "sysadmin".

### c) Administration ALCASAR in GUI mode

To remotely administer ALCASAR in GUI mode, it is necessary to redirect the data flow from the administrative station's web browser into a SSH tunnel to ALCASAR. To create the tunnel:

- On Linux, run the command:  
`ssh -L 10000:@IP_eth1_alcasar:443 -p 52222 sysadmin@w.x.y.z »`
- On Windows, configure « putty » as following:

- Load the previous session
- On the left side of the windows, select "Connection / SSH / Tunnels»
- In "Source Port" enter the port of entry of the local tunnel (greater than 1024 (here 10000))
- In "Destination", enter the IP address of eth1 of alcasar1 followed by the port 443 (here 192.168.0.1:443)
- Click on "Add"
- Select "Session" on the left side
- Click on "Save" to save your changes
- Click on "Open" to open the tunnel
- Enter the user name and password



Start your WEB browser with the URL : “https://localhost:10000/acc/”

⚠ The “acc/” in the end of URM is important!

### d) Administration of equipment on the consultation network

Following the same logic, it is possible to administer any equipments connected on the consultation network (WIFI access points, switches, LDAP / AD, etc.).

- On Linux, run the command: `ssh -L 10000:@IP_equipment:Num_Port -p 52222 sysadmin@w.x.y.z ».`  
`@IP_equipment` is the IP address of the equipment to administer. `NUM_PORT` is the administration port of this equipment (22, 80, 443, etc.).
- On Windows, enter the IP address and the port of the equipment in the form "Destination" of "Putty".

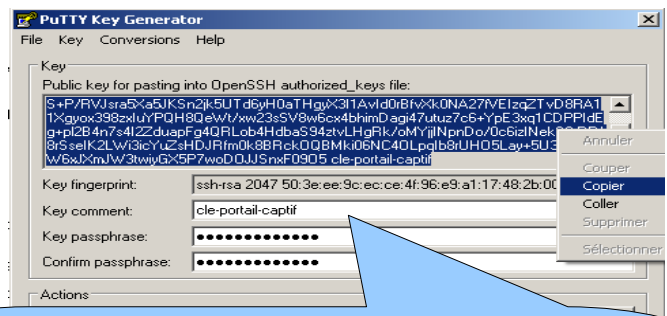
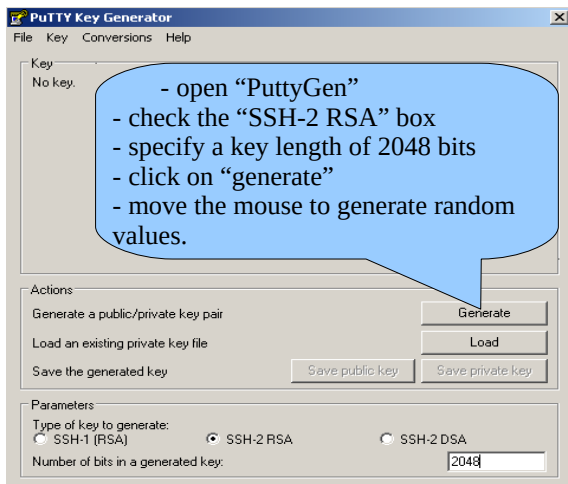
Launch : `ssh login@localhost:10000` » will provide a ssh-based remote administration.

To use a web interface, launch your browser and type the URL: `http(s)://localhost:10000` ».

### e) Use of SSH tunnel with a key pair (public/private key)

This paragraph, although not essential, add an additional layer of security using private key authentication.

- generate a keys pair (public key / private key)
  - On Windows with « puttygen »



The keys are now created.

- Linux with « `ssh-keygen` »

In your personal directory, create the directory « `.ssh` » if it is not exist. From this one, generate your public/private key pair (« `ssh-keygen -t rsa -b 2048 -f id_rsa` »). The command « `cat id_rsa.pub` » allow you to see (and to copy) your public key.

```
richard@rexy ~]$ mkdir .ssh
richard@rexy ~]$ cd .ssh/
richard@rexy .ssh]$ ssh-keygen -t rsa -b 2048 -f id_rsa
Generating public/private rsa key pair.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in id_rsa.
Your public key has been saved in id_rsa.pub.
```

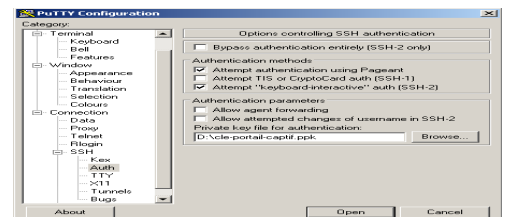
```
richard@rexy .ssh]$ cat id_rsa.pub
ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAQEAyL4yMM8B018Quusv1Iq/V
3kfF2wvhuHzmNmH9ITFTALWHPHA91Wnx1cDPE9DPR7FPqrEZF/uT84C2G3
o7d/IX-/JyP1VxOudXaZ9wjtuS3SVWSr6o9NXmbZqo0gzrGpjN7Vfu5
nPrCdQGfuuq6PIm06AQCJQkySmOXDlGFVr4r5Zbw== richard@rexy
```

- Copy the public key on the remote portal:
  - run the following command to copy your public key directly on the remote server:
    - `ssh-copy-id -i .ssh/id_rsa.pub sysadmin@<@IP_interne_consultation>`
    - Enter your password; your public key is copied in the `sysadmin/.ssh/authorized_keys` automatically with the correct permissions.
  - Another method : log on through SSH to the remote ALASAR as "sysadmin" and execute the following commands : « `mkdir .ssh` » then « `cat > .ssh/authorized_keys` » ;
    - copy the contents of the public key from the clipboard ("Ctrl V" for Windows, middle mouse button for Linux) type « `Enter` » then « `Ctrl+D` » ; protect the directory : « `chmod 700 .ssh` » and key file « `chmod 600 .ssh/authorized_keys` » ; check the file : « `cat .ssh/authorized_keys` » and log out : « `exit` ».

- Connection test from Linux host : « `slogin sysadmin@w.x.y.z` »

- Connection test from Windows host :

- load the previous session of putty;
- on the left side, select "Connection / SSH / Auth";
- click on "browse" to select the key file;
- on the left side, select "Session";
- click on "Save" then on "Open";
- enter the user "sysadmin";
- the key is recognized, it remains only to enter the passphrase.



- If now you want to prevent the connection with passphrase, configure the sshd server:

- become root (`su -`) and set the following options on the file « `/etc/ssh/sshd_config` » :
  - `ChallengeResponseAuthentication no`
  - `PasswordAuthentication no`
  - `UsePAM no`
- restart the sshd server (« `service sshd restart` ») and close the ssh session (« `exit` »).

```
richard@rexy ~]$ slogin sysadmin@
Bienvenue sur alcasar-rexy-74
Enter passphrase for key '/home/richard/.ssh/id_rsa':
Last login: Sat Apr 3 20:14:51 2010 from
alcasar-rexy-74:~$
```

### 8.3. How to display the logo of the organization

It is possible to display the logo of your organization by clicking on the logo on the upper right corner of the management interface. Your logo will be inserted in the authentication page and at the top of the page of your



management interface. Your logo must be in "png" format and its size must not exceed 100KB. It is necessary to refresh the page to see the change.

## 8.4. Use of the server certificate

ALCASAR encrypts data with equipments on the consultation network in the following cases:

- for users : authentication request and changing passwords;
- for administrators : access to graphical ALCASAR Control Center (ACC).

Encryption uses TLS protocol with a server certificate and a local certificate authority (CA) created during the installation. This server certificate has a validity of four years. You can check it on homepage of the ACC :

If the server certificate is expired, you can create a new one with the following command : « `alcasar-CA.sh` ».

Système	
Nom d'hôte canonique	alcasar
Date d'expiration du certificat	May 30 23:59:59 2012 GMT
Version du noyau	2.6.33.7-desktop586-2mnb (SMP)
Distribution	★ Mandriva Linux 2010.2
Uptime	51 minutes
Utilisateurs	1
Charge système	0.00 0.00 0.00   0%

**It will be necessary to remove the old certificate from browsers before installing the new one.**

### a) Installation of an official certificate

Since version 2.0 it is possible to install an "intranet" official certificate offer by some suppliers. The installation of such a certificate ovoids security warning dialog box in browsers which have not installed the ALCASAR root certificate (cf. §2.2.c). Unlike "Internet" certificates which certify a domain name registered at a registrar, an "intranet" certificate can certify a private IP address or a simple server name (hostname). This corresponds to the situation of ALCASAR whose "hostname" is always "alcasar" To obtain your certificate, follow the instructions as noted on the supplier's web page knowing that the web server used by ALCASAR is an "APACHE" server with a SSL module. The following example can demonstrate how installing an "intranet" certificate created by the "Digitalix" supplier.

First, you will have to execute the following command on ALCASAR as "root" :



- `openssl req -newkey rsa:2048 -new -nodes -keyout alcasar.key -out alcasar.csr`  
This command creates two files : the private key (`alcasar.key`) and the certificate request (`alcasar.csr`).
  - Copy the certificate request file on a USB flash drive in order to be able to copy its contents on the webpage of the supplier. The supplier must return you a file containing your official server certificate (`alcasar.crt`). If needed, you also have to download the intermediate authority certificate of your provider (for Digitalix, it is available here: <http://www.digitalix.fr/certs/HACert-bundle.crt>).
  - As "root", copy the three files « `alcasar.key` », `alcasar.crt` » and « `HACert-bundle.crt` » in your directory (`/root`). Then, execute the following commands :
1. `cd /etc/pki/tls` (moving in the certificate directory)
  2. `mv certs/alcasar.crt certs/alcasar.crt.old` then `mv certs/server-chain.crt certs/server-chain.crt.old` and finally `mv private/alcasar.key private/alcasar.key.old` (backup of the old certificates)
  3. `cp /root/alcasar.crt certs/` et `cp /root/alcasar.key private/` (copy of the official certificate and of its private key)
  4. if your supplier owns a intermediate authority certificate: `cp /root/HACert-bundle.crt certs/server-chain.crt` else : `cp certs/alcasar.crt certs/server-chain.crt`
  5. Restart the Apache Web server with the command « `service httpd restart` ».

If you're having problems:

- either you reverse the instructions of the second line; or you create new local certificates again with the command : « `alcasar-CA.sh` » ;
- restart the Apache Web server with the command : « `service httpd restart` ».

### b) Copy of a certificate on several ALCASAR server

If you use several ALCASAR server, it may be interesting to copy the certificate from a reference ALCASAR to other ALCASAR. If you installed an official certificate, execute the commands from the points 1 to 5 from the previous section on the differents ALCASAR. In the case of a certificate created during installation, copy the five following files from the reference ALCASAR to the other servers:

- for the certification authority : `/etc/pki/CA/alcasar-ca.crt` and `/etc/pki/CA/private/alcasar-ca.key`

- for the server certificate : `/etc/pki/tls/certs/alcasar.crt`, `/etc/pki/tls/certs/server-chain.crt` and `/etc/pki/tls/private/alcasar.key`

Restart the Apache Web server with the command : « `service httpd restart` ».

## 8.5. Use of an external directory server (LDAP or AD)

ALCASAR contains a module capable of requesting an external directory server (LDAP or AD) located either on the LAN side or on the WAN side.

When this module is enabled, ALCASAR uses the external directory to authenticate a user, but, if an error occurs, the local database will be used.

In all cases, user events logs are recorded in the local database of ALCASAR. Here is the management GUI of this module :

### Remark :

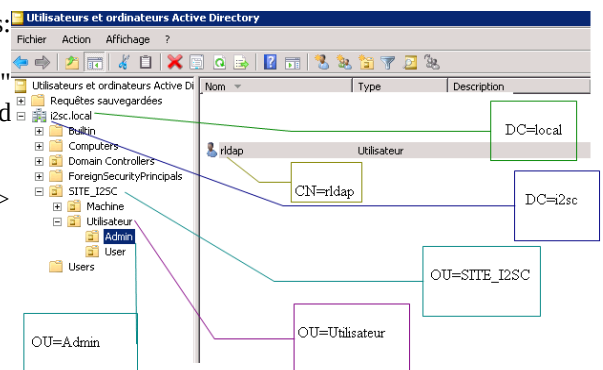
- attributes of users from the external directory can't be modified with the ACC;
- use of the secure protocol "ldaps" is not available for now. The network segment between ALCASAR and the directory server must be under control, for obvious reasons of security (cf. § 10);
- External directories do not support case sensitive unlike the local database of ALCASAR.

**Example:** This screenshot shows the AD directory tree organized as follows: standard users are put into the Organizational Unit (O.U.) "User".

The account used by ALCASAR to request the directory is the account "rldap" in the OU "Admin". This account is a standard account that does not need special rights.

Both O.U. "Admin" and "User" are located themselves in the OU "User".

- DN of the database : « `ou=User,ou=Utilisateur,ou=site_i2sc,dc=i2sc,dc=local` » --> research base of users, and this root is to be adapted to the organization of the directory tree.
- LDAP ID : « `sAMAccountName` » --> for AD; uid in general for other LDAP
- Filter : leave this field empty unless you want to select only specific users.
- LDAP user : « `cn=rldap,ou=Admin,ou=site_i2sc,dc=i2sc,dc=local` »
- Password : password of the user « rldap »



In order to provide to users from the LDAP (or AD) server, some attributes specific to ALCASAR (bandwidth, concurrent session, etc.), it is possible to create a group named "ldap" (be careful to match the case) for which you set the desired attributes.

It is also possible to assign attributes to a particular account authenticated on an external directory. To do this, create a user in the ALCASAR database with the same name / identifier as that is in the directory.

## 8.6. Integration in a complex architecture (AD, external DHCP, LDAP)

ALCASAR can be integrated into an existing architecture with a Windows domain, a DHCP server and an external directory for the authentication process (LDAP or AD) (see previous §).

### a) Windows DNS Management

If your existing environment already has Active Directory enabled, then, Windows computers of your domain controller must request the DNS of this controller for specific resolutions of the domain and they must request ALCASAR for Internet access. One solution is to configure the ALCASAR DNS so it redirects to the domain controller, DNS queries concerning resolution of the domain. In this way, devices are configured with a unique DNS : ALCASAR.


On ALCASAR, the only change to make is to add the following line in the file `<< /usr/local/etc/alcasar-dns-name >>` :

```
'server=/<your.domain>/<@IP_SRV-AD-DNS>'
```

**Example** : “brock.net” domain is managed by the AD/DNS server “192.168.182.10”. The line to add is :  
`“server=/brock.net/192.168.182.10”`

Please note that it is the domain name and not the name of the server “srv-ad.brock.net”.

Restart the service DNSMASQ to take your changes into account (`<< service dnsmasq restart >>`).

 **Reminder** : computers integrated into a Windows domain must have their DNS suffix 'localdomain' filled in (whether in static IP address mode or in DHCP mode).

### b) Using an External DHCP Server

The use of an external DHCP server requires that ALCASAR not provide the network settings, but they will be provided by a DHCP server responding to the pressing needs of ALCASAR.

To force the supply of IP addresses from an external DHCP server, ALCASAR will act as a relay agent to it. You should stop the DHCP server ALCASAR (via the management interface/System/Network: mode without DHCP) and modify variables to manage the external server (configuration file `<< /usr/local/etc/alcasar.conf >>`) :

- EXT\_DHCP\_IP=<@IP\_srv\_external>
- RELAY\_DHCP\_IP=<@IP\_internal\_ALCASAR>
- RELAY\_DHCP\_PORT=<relay port to the external DHCP server> : (default 67)

The external DHCP server must be configured to provide stations:

- a range of IP @ corresponding to the range allowed by ALCASAR (default 192.168.182.3-254/24)  
Warning: since version 2.7, the portal provided the following address that his inner interface:  
192.168.182.1 ---> the @ IP 192.168.182.2 is also reserved for the portal, but not visible.
- gateway address corresponding to the internal IP address of ALCASAR (default 192.168.182.1);  
DNS suffix "localdomain";
- the @ DNS server IP -> IP address internal ALCASAR (default 192.168.182.1);
- the @ IP of the time server (NTP) -> the internal IP address of ALCASAR (default 192.168.182.1) or the domain controller (to avoid temporal drifts, also to ensure the implementation position automatic time therefor to a server matched to the Internet or more simply ALCASAR).

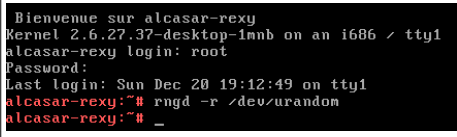
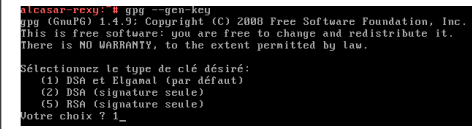
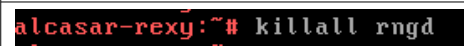
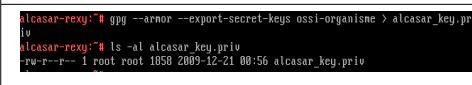
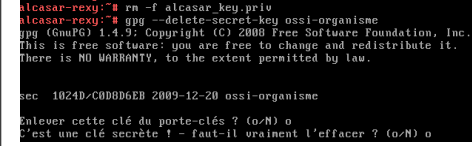

## 8.7. Encryption of log files

ALCASAR can automatically encrypt the weekly archive files (see §7.1). To perform this, it uses the asymmetric algorithm (GPG public key + private key).

Providing the private key to a responsible body (ie : CISO), you protect your administrators to be accused of having change the content of these log files.

In case of judicial inquiry, simply provide log files and encrypted private key for decryption.

The procedure for activating the encryption is as follows:

Printscreen	Comments	To do
	- Log on as « root ». - Start the entropy generator.	<code>rngd -r /dev/urandom</code>
	- Generate the key pair (public key + private key). - Choose the algorithm, the size and durability of the keys (no expiration). - Choose a user name and passphrase.	<code>gpg --gen-key</code>  info: The user name must not contain spaces. This name is included under the term <username> later in this procedure.
	- Stop the entropy generator.	<code>killall rngd</code>
	- Export the private key. Copy this to an external media. - Give it (with passphrase and username) to an official of your organization (for receiver).	<code>gpg --armor --export-secret-key \ &lt;username&gt; &gt; alcasar_key.priv</code>  info : cf. installation doc for the USB management.
	- Delete the previously generated keys - Delete the private key from GPG keyring	<code>rm -f alcasar_key.priv</code>  <code>gpg --delete-secret-key &lt;nom_utilisateur&gt;</code>
	- Enable encryption by changing <b>the</b> variables "CRYPT" and "gpg_user" in the file « /usr/local/bin/alcasar-archive.sh ».	<code>vi /usr/local/bin/alcasar-archive.sh</code>  info : assign the "username" to the variable « gpg_user »

### Infos :

- ALCASAR uses the keyring "root" in the directory « /root/.gnupg » ;
- '`gpg --list-key`' : allows to list all the key pairs contained in this kit;
- '`gpg --delete-key <user_name>`' : deletes a public key keyring;
- '`gpg --delete-secret-key <user_name>`' : deletes a private key keyring;
- You can copy the directory « /root/.gnupg » on another server ALCASAR. Thus, you can use the same key and the same <username>;
- To decipher an encrypted archive: '`gpg --decrypt <filename_crypt_archive>`'.



## 8.8. Managing multiple Internet connections (load balancing)

ALCASAR has a script to distribute connections to multiple gateways to the Internet "`alcasar-load_balancing.sh start | stop | status`".

The parameters are not included in the management interface, it is necessary to modify the global configuration file "`/usr/local/etc/alcasar.conf`".

Associated parameters (cards of virtual networks, weights, @ ip gateway, etc.) are defined in the following format : `WANx = "active [1 | 0], @ IPx / mask, GWx, Weight, MTUX"`.

Interfaces are created on the fly by the script. To be active, the MULTIWAN parameter must include the "on" value or "On" position if the "Off" mode to keep "single gateway".

The frequency of the connectivity test is set by default to 30sec.

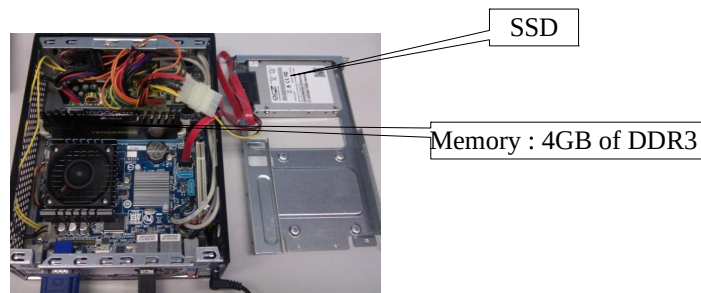
Note that a value of the "FAILOVER=0" indicates a test mode without MULTIWAN connectivity gateways.

## 8.9. Creating a dedicated housing (appliance) ALCASAR

This chapter presents an example of an assembly of a low-cost dedicated housing (appliance) ALCASAR with the following constraints : small form factor (mini-itx), low noise and low power consumption.

Here is the hardware list :

- PC Case mini ITX (12V powerline);
- motherboard GigaByte GA-C847N (with two integrated network cards and Intel Celeron C847);
- 4GB of DDR3 memory;
- HDD 2.5' 200GB SATA.



The cost of this configuration is nearly 250 € (including postage).

The power consumption of this mini-PC is not more than 30W; the cost of the annual electricity consumption in France is about 30€ ( $30 * 24 * 365/1000 * 0.1329$ ).

ALCASAR is installed via a USB drive as usual.

Once installed, the appliance does not need any keyboard, mouse and screen anymore.

## 8.10. Portal by-pass

For maintenance or emergency reasons, a portal by-pass procedure has been created.

It allows to felete authentication of the users as well as filtering. However, the network events logging remains active, but the imputability of the connexions is not ensure anymore.

- To execute the portal by-pass, execute the script « `alcasar-bypass.sh --on` ».
- To stop it, execute the script « `alcasar-bypass.sh --off` ».

It should be noted that the bypass is no longer active when the server restarts.

## 9. Shutdown, updates and reinstallation

### 9.1. Shutdown

Two ways exist to shutdown properly the ALCASAR portal :

- by briefly pressing the power button of the computer;
- by logging in on the console as root and by executing the command "systemctl poweroff";

When restarting the portal ALCASAR a script deletes all the connections that have not been closed after an undesired shutdown (hardware problem, power failure, etc.).

### 9.2. Updates of the operating system

Mageia-Linux provides an excellent mechanism to apply security updates (patches) on the system and its components. ALCASAR has been developed in order to be fully compatible with this mechanism. So, every night at 3:30 AM, security updates are downloaded, authenticated and applied if necessary. Of course, it is possible to execute this update manually with the command « `urpmi -auto --auto-update` » as « root ».

Once the update is completed, a message may warn you that reboot of the computer is necessary. This message only appears if a new kernel (kernel) or a major library were updated.

### 9.3. ALCASAR updates

You can check if an update of ALCASAR is available on the home page of the ACC or by executing the following command « `alcasar-version.sh` ». Download and extract the latest version as if it was the first installation of ALCASAR. Run the installation script (« `sh alcasar.sh --install` »), it will automatically detect the previous version and ask if you want to perform an update. During an update, the following settings will still remain :

- network configuration;
- the name and logo of the organization;
- logins and passwords of the administrators accounts;
- users and groups database;
- main and secondary blacklist;
- trusted sites and MAC addresses list;
- network filtering configuration
- certificate of the Certification Authority (CA) and certificate of the server.

### 9.4. Reinstallation of a portal

ALCASAR integrates a mechanism to reinstall the portal with its settings. This is useful if you change the server (hardware update, hardware failure, etc.). Generating a portal configuration archive from the ACC (see §7.3). Copy the archive on a USB flash drive. Install the new operating system as if it was an initial installation. Plug the USB flash drive and copy the archive file in the « `/tmp` » directory. Download and extract the latest version of ALCASAR and install it as if it was a first installation: « `sh alcasar.sh --install` ».

## 10. Troubleshooting

If you have problem with ALCASAR, this chapter sets out several troubleshooting steps that may indicate the cause. All commands (italic test on a yellow background) must be run in a console as "root".

### 10.1. Network connectivity

- **test the status of the network cards** : run the commands « `ethtool eth0` » and « `ethtool eth1` » in order to check the status of both network cards ( fields "`Link detected`" and "`Speed`" for example ) ;
- **gateway/broadband-router connexion test** : "`ping`" the router @IP. If an error occurs, check the cable connexion, the eth0 settings (`ifconfig eth0`) and the status of the gateway / broadband-router;
- **external DNS servers connexion test** : « `ping` » the DNS server. If an error occurs, try another servers;
- **internal DNS server (dnsmasq) connexion test** : send a name resolution request (ex. : `dig www.google.fr`). If an error occurs, check the configuration file of "dnsmasq" (`cat /etc/dnsmasq.conf`).

In order to check the proper operation of the service or the redirections (in the case of an internal DNS server), uncomment the first line OPTIONS in the file `/etc/sysconfig/dnsmasq` to display the requests and their responses (`tailf /var/log/dnsmasq/queries.log`). But be aware, this is very resource-intensive. So don't forget to comment it again. Finally, to be take changes into account, you need to restart dnsmasq service : « `service dnsmasq restart` » ;

- **connexion test to Internet**: run the command « `wget www.google.fr` ». If successful the front page of Google is downloaded and stored locally (index.html). The "system / service" menu of ACC reports this test;
- **consultation equipment connexion test** : you can check if an equipment is connected to the consultation network by running the command « `arping -I eth1 @ip_quipment` ».



To discover all equipments connected on the consultation network, run the command « `arpscan eth1` » ;

`00:1C:25:CB:BA:7B 192.168.182.1`  
`00:11:25:B5:FC:41 192.168.182.25`  
`00:15:77:A2:6D:E9 192.168.182.129`

You can display the network packets coming from the consultation by installing the « `tcpdump` » tool (`urpmi tcpdump`) and by running the command : « `tcpdump -i eth1` ».

### 10.2. Available disk space

If the available disk space is not enough, some modules may not run properly. For example, the proxy server "Squid" swill tops working as soon as it will not be able to write its log. You can check the available disk space (especially /var partition) :

Point	Type	Partition	Utilisation	Libre	Occupé	Taille
/	ext3	/dev/sda1	59% (1%)	383.34 Mo	547.34 Mo	980.49 Mo
/tmp	ext3	/dev/sda6	3% (1%)	1.83 Go	33.77 Mo	1.12 Go
/home	ext3	/dev/sda7	3% (1%)	1.87 Go	33.46 Mo	1.10 Go
/var	ext3	/dev/sda8	0%	62.74 Go	251.01 Mo	66.35 Go
			Totaux : 11%	65.21 Go	865.59 Mo	69.53 Go

- in GUI mode with the homepage of ACC;
- in text mode, with the command « `df` »

In case of excessive reduction of this space, delete old log files after they have been archived (directory `/var/Save/*`).

### 10.3. Server services

In order to compete these tasks, ALCASAR uses several server services. If one of them stops, ALCASAR would stop running too. It's useful to know why and how a service stopped. On a text console, run the command « `ps fax` » and check that the web server apache ("httpd") is still running. If not, start it with the command « `service httpd start` ». If an error occurs, display its log with the command « `tailf /var/log/httpd/error.log` ». If "apache" is running, you can access of the operating status of the other services in the ACC (menu « System/Services ») :

Status	Nom du services	Actions
✓	radiusd	--- Arrêter Redémarrer
✓	chilli	--- Arrêter Redémarrer
✓	dansguardian	--- Arrêter Redémarrer
✓	mysqld	--- Arrêter Redémarrer
✓	squid	--- Arrêter Redémarrer

You can stop or restart them through the ACC or with the command "service service\_name start / stop / restart". If an error occurs, check in the system log file (`tailf /var/log/messages`) the reason why it does not work.

### 10.4. Connectivity of the clients

In the ACC ("System / Activity"), make sure that client' network settings are correct (MAC address / IP address). If this is not the

#	adresse IP	adresse MAC	usager	Action
1	192.168.182.130	00-0B-6C-3A-55-4D	██████	Déconnecter
2	192.168.182.22	00-1A-A0-2F-10-DB	██████	Déconnecter
3	192.168.182.15	00-15-58-B7-24-BA	██████	Supprimer
4	192.168.182.10	00-15-58-B7-5B-22	██████	Déconnecter

case, delete the old settings registered by ALCASAR and reconfigure the client equipment.

On the client :

- check the network settings : run « `ipconfig /all` » on Windows, « `/sbin/ifconfig` » on Linux ;
- if they are not correct, update them. For device that use dynamic IP addresses, send again an DHCP request : « `ipconfig /renew` » on Windows, « `dhclient eth0` » on Linux.

If the interface is not configured, check the cables connections and make sure that DHCP frames flow on the network (use the network analyzer "wireshark" for example). On ALCASAR, you can see incoming DHCP requests by running the command « `tailf /var/log/messages` » or by displaying the terminal 12 (<Alt> + F12).

```
Dec 29 22:31:27 alcasar coova-chilli[2299]: chilli.c: 2694: New DHCP request from MAC=08-00-27-E7-EA-89
Dec 29 22:31:27 alcasar coova-chilli[2299]: chilli.c: 2661: Client MAC=08-00-27-E7-EA-89 assigned IP 192.168.182.129
```

- Connection test to the portal : send a ping request to the IP address of ALCASAR. If an error occurs, check the cable connection and the network interface settings.
- Name resolution test : On Windows, run « `nslookup alcasar` ». On Linux, run « `dig alcasar` ». The result must be the IP address of ALCASAR. If not, check that the IP address of ALCASAR is the DNS server IP address of the client.
- ACC test : Open a browser on a client and try to connect to ALCASAR (`http://alcasar`).
- Internet Connection test : Try to visit a Internet website with the HTTP protocol (no HTTPS!). ALCASAR must "intercept" you and display the authentication window.

## 10.5. Connection to ALCASAR with a serial terminal

It may be useful to let the ALCASAR server without a screen and keyboard. Below is a short tutorial to connect a serial terminal (thank you [Igor Popowski](#)) :

<p>File <code>/etc/inittab</code> :</p> <ul style="list-style-type: none"><li>• save the original : <code>cp /etc/inittab /etc/inittab.save</code></li><li>• edit the file : <code>vi /etc/inittab</code> before this line : « # Single user mode », add the following lines: <code>#connexion au terminal serial</code> <code>s0:2345:respawn:/sbin/agetty -L 9600 ttyS0 vt100 -f /etc/issue</code> then save « Esc » then « :wq! »</li></ul>	<p>File <code>/etc/securetty</code> :</p> <ul style="list-style-type: none"><li>• save the original : <code>cp /etc/securetty /etc/securetty.save</code></li><li>• edit the file : <code>vi /etc/securetty</code> add one of the two following line at the end of file: <code>ttyS0</code> if using a 9-pin serial port <code>ttyUSB0</code> if using a Serial / USB and save « Echap » and « :wq! »</li><li>• run the command « <code>init q</code> » to account for this change.</li></ul>
<p>To see the output of the boot in GRUB, edit the file <code>/boot/grub/menu.lst</code></p> <ul style="list-style-type: none"><li>• save the original: <code>cp /boot/grub/menu.lst /boot/grub/menu.lst.save</code></li><li>• in the section 'title linux' after adding <code>vga=791</code> to end of line : <code>console=tty0 console=ttyS0,9600n8</code> by standard serial port <code>console=tty0 console=ttyUSB0,9600n8</code> in USB port</li></ul>	

Connect a PC with a null modem cable to the serial port com1 of ALCASAR (or via a serial / USB adapter). Setup "putty" to use this serial com1 in vt100.

## 10.6. Troubleshooting

This chapter presents feedbacks of organizations who have solved identified problems.

### a) On some sites, pictures are not displayed

When domains name and URLs filtering is enabled, by default, ALCASAR filters web links without domain name (leading to IP addresses). Thus, the pages containing this kind of links are partially displayed. To prevent from this problem, two solutions : remove the "IP" blacklist (cf. § 5.1.c) or record the IP addresses contained in these links as "domain name rehabilitated" (cf. § 5.1.c). For example, the site "leboncoin.fr" hosts its pictures on the following IP addresses: 193.164.196.30, .40, .50 and .60 and 193.164.197.30, .40 and .50.

### b) No Internet browsing with some antivirus

Disable the "web-proxy" integrated in some antivirus (ie: trend-micro). This function uses a white/black list which is available on Internet servers (backup30.trendmicro.com, etc..). To avoid problem that may be incompatible with the ALCASAR embeded proxies, stop the service "Trend Proxy Service" and restart the client computer.

### c) Windows client previously connected to a public hotspot

When a system connects to a "public hotspot", it provides network parameters as well as "lease time" which determines the length of time an IP address remain assigned. Windows XP clients do not reset these settings during a reboot.

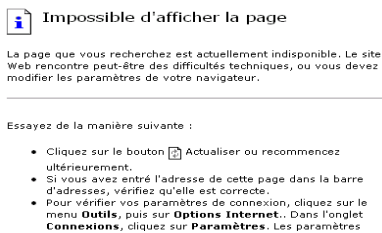
So, even if they change of network, they will try to connect with the previous settings. This problem is recognized by Microsoft that offers the following solution : manually force the refreshing of the IP address with the command : « `ipconfig /renew` ».

### d) Windows client with static addressing

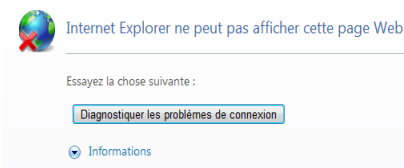
It is necessary to add the DNS suffix "localdomain" (network configuration / advanced / DNS tab).

### e) No Internet browsing although the browser accesses the ALCASAR homepage

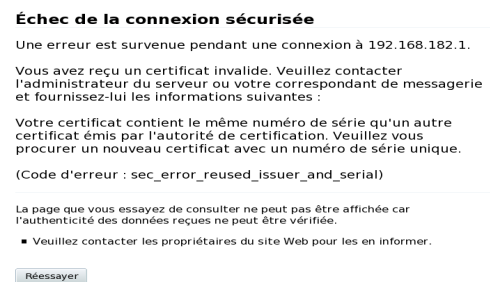
This can occur after a complete reinstallation of the portal or after an update with a change server certificate. Browsers display the following pages when they try to access a website:



With IE6



With IE 7 - 8 and 9



With Mozilla

This is because browsers try to authenticate the ALCASAR portal using an old certificate. The old certificate must be removed ("tools" + "Internet Options", tab "content" button "Certificates" tab "root certification authorities") to replace the latter as described in § 2.2.c

### f) No Internet browsing after filling the "trusted sites" section

ALCASAR verifies the validity of the domain names entered in the section (cf. § 4.7.a). If a domain name is not valid, the 'chilli' service can't start. So, modify the invalid domain name and restart the 'chilli' service via the command « `service chilli restart` ».

## g) Overload memory and system

The Linux system always tries to exploit the maximum of RAM. On the home page of ACC, a bargraph display the use of physical memory. It can regularly be found beyond 80% and appear red. This is normal. If the system needs more memory, it will use the swap. This swap is an area of the hard disk operates as RAM (but 1000 times slower). If you find that the system uses swap space (> 1%), you can consider that increasing the RAM will improve the system responsiveness (especially when the DNS domain filter module is enabled).

You can view the system load on the ACC homepage, or in a console with the command « `top` » or « `uptime` » :

- The 3 values represent the system load average for the last 5 and last 15 minutes. The load average is the number of processes waiting for CPU usage. These values are normally less than 1.
- A value greater than '1.00' results under-sizing of the server (especially if it affects the three values (payload included in the length).
- Search process that monopolizes a large percentage of the load (command « `top` »).

## 11. Security

On consultation network, ALCASAR is the way to control Internet access. It also helps protect the network against an exterior pirate. To do this, it includes:

- a protection against identifiers theft. The authentication flows between client and ALCASAR are encrypted. The passwords are stored encrypted in the database;
- a protection against disconnection omissions. The attribute "time limit of one session" (cf. § 3.1) allows a user to disconnect automatically after a set time;
- a protection against sleep clients. Users whose equipment does not respond for 6 minutes are automatically disconnected;
- a protection against session hijacking (parameters spoofing). This spoofing method uses the weaknesses of "Ethernet" and WIFI protocols. To reduce this risk, ALCASAR launch a process every 3 minutes (`alcasar-watchdog.sh`). This process disconnected the spoofed users ;
- a protection of the bootloader (grub) with a password. This password is stored in the file « `/root/ALCASAR-passwords.txt` ».

The presence of ALCASAR doesn't guarantee the absolute security against all threats, including the internal threat (pirate on the consultation network).

In most cases, this threat remains very low. Without being paranoid, if you need high security, the following checks can improve the overall security of your system.

### 11.1. On ALCASAR

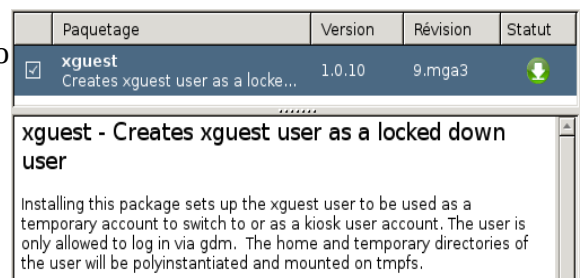
- Choose a robust "root" password (you can change it by running the command « `passwd` ») ;
- Protect the ALCASAR PC and the ISP's equipment to prevent unauthorized access, theft or installation of equipment between the broadband router and ALCASAR (locks, etc.).
- configure the BIOS so that only the internal hard disk is bootable.
- Set a password to access the BIOS setup.

### 11.2. On the consultation network

#### a) Open networks

If you want to set up free access computers, it may be interesting to install products ensuring both the protection of the privacy and security (like "cybercafe" computers) . These products allow the user to be partitionned in a sealed environment. At the end of his session, the user environment is totally cleaned.

- With Linux, you can install the product "xguest" (it is provided natively on Mageia, Mandriva, Fedora, RedHat and Centos)
- With Windows, Microsoft gave the software "Steady state" for XP/Vista. This software is no more supported.



These networks often use WIFI. On the access points (AP), enable WPA2 encryption "personal." This avoids user to listen WIFI traffic (even if the key is the same for everyone). You can choose a simple WPA2 key as your organization name for example.

With Ethernet switches, enable "DHCP snooping" on ALCASAR port and on interswitch ports. This will prevent false (fake) DHCP servers.

### **b) Controlled networks**

On these networks, the stations must be protected by physical measures to ensure their integrity. Physical access to network consultation must be secured by the following:

- disconnect unused network jacks;
- on WIFI hotspots:
  - camouflage the network name (SSID)
  - enable encryption WPA2 "personal" with a robust key;
- on Ethernet switches:
  - Enable the "lock port" (function "Port Security") to associate the MAC addresses of devices to the physical ports of switches;
  - select the "DHCP snooping" on port operated by ALCASAR well as the interswitch ports. This will prevent false DHCP servers (Fake DHCP servers).

Consultation computers can (should) incorporate several security features such as locking the BIOS setup and office, antivirus, automatic update security patches (patch), etc. To facilitate downloading security patches or updated antivirus (cf. § 4.7), ALCASAR may authorize equipment to automatically connect without authentication on sites specifically identified.



**Educate users to change their password and they do not disclose their identifiers (they are responsible sessions a "friend" to whom they have supplied).**

## 12. Annexes


### 12.1. Useful commands and files

The administration of ALCASAR is used directly in a terminal command line (as 'root'). All these commands start with "alcasar-... ". All these commands (shell scripts) are located in the directories « [/usr/local/bin/](#) » and « [/usr/local/sbin/](#) ». They often use the central configuration file of ALCASAR (« [/usr/local/etc/alcasar.conf](#) »). With the “-h” argument, each command lists its options.

- `alcasar-bl.sh {-on/-off}` : enables / disables the filtering domains and URL;
  - `{-download}` : download and apply the latest version of the BlackList Toulouse;
  - `{-adapt}` : adapt the BL to ALCASAR architecture ;
  - `{-reload}` : activate the BL freshly downloaded.
- `alcasar-bypass.sh {-on/-off}` : active mode on / off « BYPASS » ;
- `alcasar-CA.sh` : creates a local CA and server certificate. Requires restarting the Apache web server (`service httpd restart`) ;
- `alcasar-conf {-apply}` : apply the network settings according to the configuration file;
- `alcasar-dg-pureip.sh {-on/-off}` : enables / disables the filtering of URLs containing IP addresses (instead of a domain name);
- `alcasar-havp.sh {-on/-off}` : enables / disables the antivirus filtering flows WEB;
  - `{-update}` : am updating the knowledge base of antivirus(clamav) ;
- `alcasar-https.sh {-on/-off}` : enables / disables the encryption authentication flow;
- `alcasar-load-balancing.sh` : script for aggregating several distinct internet. To function, the file “[/usr/local/etc/alcasar.conf](#)” must be set to take into account the addresses, the number and weight of bridges (box) available. This script is run automatically when the server starts but is only active if the MULTIWAN parameter is set to “[/usr/local/etc/alcasar.conf](#).” To verify proper operation, run the command: `ip route`. The options are start, stop and status.
- `alcasar-logout.sh {username}` : disconnect users <username> all its sessions;
  - `{all}` : disconnects all connected users;
- `alcasar-mysql.sh {-import fichier_sql.sql}` : imports a user base overwrites the existing
  - `{-raz}` : reset the user base;
  - `{-dump}` : create an archive of the current user base in « [/var/Save/base](#) » ;
  - `{-acct_stop}` : stopsessions open accounts;
- `alcasar-nf.sh {-on/-off}` : enables / disables the filtering of network protocols;
- `alcasar-rpm-download.sh` : compares the version ALCASAR active with the latest version available on the Internet;
- `alcasar-safesearch.sh {-on/-off}` : active/désactive le filtrage « mineur » major search engines;
- `alcasar-version.sh` : compares the version ALCASAR active with the latest version available on the Internet;

Each service provided by the server is supported by a "daemon", which is managed automatically start:

- View the status of a particular daemon (works for most daemons)  
`/etc/init.d/<nom du service> status`
- Restart / stop a daemon:  
`/etc/init.d/<nom du service> {start|stop|restart|reload}`

 **Info** : a super daemon checks every 10 minutes service status (“`alcasar-daemon.sh`”).

If you need to edit a file, you'll probably need to know some basic features of the text editor "vi". You can then carefully press you a summary of common commands on the site: [http://wiki.linux-france.org/wiki/Utilisation\\_de\\_vi](http://wiki.linux-france.org/wiki/Utilisation_de_vi) .

Sauvegarder un fichier - quitter vi	
:w	sauvegarde le fichier (penser à write)
:wq	sauvegarde le fichier et quitte vi (write and quit) équivalent à :x
:q	quitte vi sans sauvegarder les modifications (quit)
:q!	quitte immédiatement, sans rien faire d'autre
:w <nom_de_fichier>	sauvegarde le fichier sous le nom <nom_de_fichier>
:w	sauvegarde le fichier (penser à write)
:wq	sauvegarde le fichier et quitte vi (write and quit) équivalent à :x
:q	quitte vi sans sauvegarder les modifications (quit)
:q!	quitte immédiatement, sans rien faire d'autre
:w <nom_de_fichier>	sauvegarde le fichier sous le nom <nom_de_fichier>

Copier-Coller	
Y	copie une ligne, donc la place dans un tampon, pour pouvoir ensuite la coller (yank, tirer)
nY	copie n lignes
p	colle les lignes après le curseur (paste, coller)

Annuler ou répéter des modifications	
u	annule la dernière modification (undo, défaire) (un point) répète les dernières modifications

Insérer du texte	
i	active le mode insertion

Supprimer du texte	
x	supprime un caractère (« faire une croix dessus »)
dd	supprime une ligne
n dd	supprime n lignes

Rechercher et remplacer	
/motif	recherche motif en allant vers la fin du document
n	répète la dernière recherche (next, suivant)
N	retourne au résultat de la précédente recherche effectuée
:%s/motif/motif2/g	recherche le motif et la remplace par motif2



## 12.2. Authentication exceptions helpful

The following values allow network devices to access WEB sites without authentication process in order to connect to the following services:

- testing connectivity of the Internet,
- updated Microsoft system,
- update “TrendMicro” and “clamav” antiviruses,
- test client version of mozilla and its modules,
- ...

Sites, @ IP or URLs are configurable through the management interface or directly in the following file “*/usr/local/etc/alcasar-uamallowed*”:

```
uamallowed="activation.sls.microsoft.com"  
uamallowed="www.msftncsi.com"  
uamallowed="crl.microsoft.com"  
uamallowed="download.microsoft.com"  
uamallowed="download.windowsupdate.com"  
uamallowed="go.microsoft.com"  
uamallowed="ntservicepack.microsoft.com"  
uamallowed="stats.update.microsoft.com"  
uamallowed="update.microsoft.com"  
uamallowed="update.microsoft.com.nsatc.net"  
uamallowed="pccreg.trendmicro.de"  
uamallowed="pmac.trendmicro.com"  
uamallowed="tis16-emea-p.activeupdate.trendmicro.com"  
uamallowed="update.nai.com"  
uamallowed="download.mozilla.org"
```

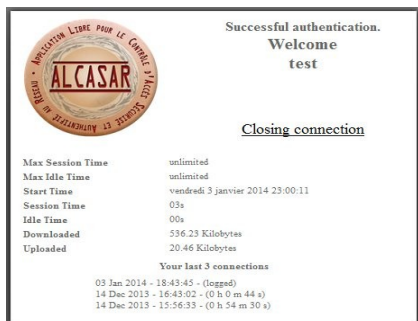
Domains are also configurable via the management interface or directly in the following file:

```
“/usr/local/etc/alcasar-uamdomain”:  
uamdomain=".download.microsoft.com"  
uamdomain=".download.windowsupdate.com"  
uamdomain=".ds.download.windowsupdate.com"  
uamdomain=".microsoft.com"  
uamdomain=".update.microsoft.com"  
uamdomain=".update.microsoft.com.nsatc.net"  
uamdomain=".windowsupdate.com"  
uamdomain=".windowsupdate.microsoft.com"  
uamdomain=".trendmicro.com"  
uamdomain=".activeupdate.trendmicro.com"  
uamdomain=".akamaiedge.net"  
uamdomain=".akamaitechnologies.com"  
uamdomain=".clamav.net"
```

It is necessary to restart the “chilli” service, if the files are manually changed.

## 12.3. Sheet of User

Internet access control has been implemented through a portal ALCASAR. When you try to connect to the Internet, the following login window is displayed. Be careful, the fields are case sensitive ("smith" and "Smith" are two different users).

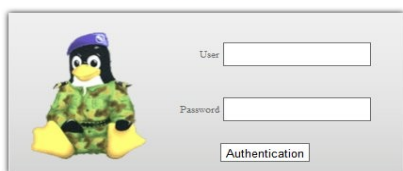


When authentication is successful, the following window "pop-up" is displayed. It allows you to disconnect from the portal (closing connection). This window provides information on the rights granted to your account (expirations, download limits, list of last 3 sessions, etc.).

If this window is closed when you want to disconnect, simply enter "http://logout" in the URL of your browser.

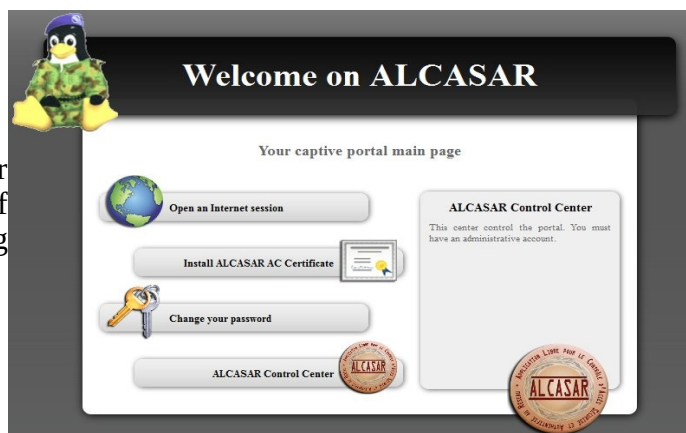
### Access Control

Authentication Failed  
your account expired



If connection fails, a message shows the reason: Account expired, download maximum volume reached, attempting to connect outside of the allowed time slots, etc.

You can display the administration interface of your account (login/logout, change your password, integration of ALCASAR security certificate in your browser) by entering "http://ALCASAR" in the URL of your browser.



The portal embeds an anti-malware protection for the WEB flows. It embeds also a sites filtering system whose content may be objectionable. It also helps to know when the Internet connection does not work (broadband router failure or operator link failure). The following pages are displayed:

