USER MANUAL

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

Project : ALCASAR	Author : Rexy and 3abtux with support of « ALCASAR Team ». Thanks to the main translator (Clément).
Object : User manual	Version : 3.
Keywords : captive portal, access control, accountability, traceability, authentication	Date : 2018 August

Table of contents

1. <u>Introduction</u>

ALCASAR is a free and open-source Network Access Controller (NAC). This paper describes how to use it and how to administer it.

The following screenshot is displayed for users attempting to access **an HTTP** website. This page is available in English, Spanish, German, Dutch, French, Portuguese, Arabic and Chinese depending on the browsers settings. As long as the user is not logged in, no traffic will pass through ALCASAR.

The homepage of the portal is available for any browser connected on the network. By default, the URL is http://alcasar.localdomain. From there, users can log on, log out, change their password and install the security certificate into their web browsers.

Administrators can access the graphical ALCASAR Control Center (A.C.C) by clicking the little notched wheel at the bottom right of the page (or via https://alcasar.localdomain/acc/).
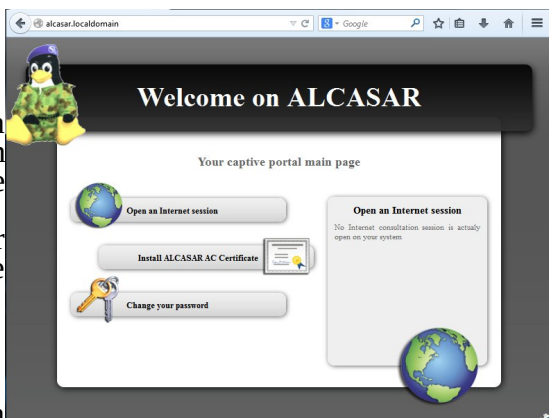
This ACC is available in two languages (English and French) via an encrypted flow (HTTPS). An authentication is required with a login name in one of the three following profiles (cf. §7.1) :

- profile « admin » can use all the administration functions ;
- profile « manager » is limited to user management functions ;
- profile « backup » is limited to a backup (of the log files) function.
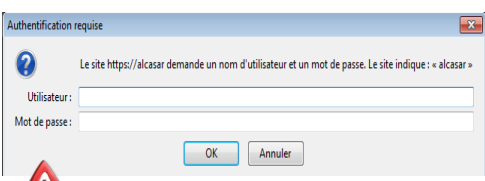
Warning : The intrusion detection system of ALCASAR will forbid new connection attempts during 3' if it detects three connection failures on ACC.

2. Network settings

On the ALCASAR network, devices can be connected with multiple technologies (wired Ethernet, Wi-Fi, PCL, etc.). For all these devices, ALCASAR is the DNS, the time server and the default gateway.

> ⚠ **CAUTION : On the consultation network, no other gateway (router) should be present. Verify the WIFI Access Points settings that must be in "bridge" mode.**

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

<u>For example, with a class C network (default configuration)</u>
- Network IP Address : 192.168.182.0/24 (sub-net mask : 255.255.255.0) ;
- Max number of devices : 253 ;
- IP address of the internal network card of ALCASAR : 192.168.182.1/24 ;
- Parameters of connected devices :
    - available IP addresses : between 192.168.182.3 and 192.168.182.254 (static or dynamic) ;
    - DNS server address : 192.168.182.1 (IP address of the internal network card of ALCASAR) ;
    - DNS suffix : localdomain <u>(this DNS suffix must be set in the static address setting of the client device)</u> ;
    - Default gateway IP address : 192.168.182.1 (IP address of the internal network card of ALCASAR) ;
    - network mask : 255.255.255.0

2.1. ALCASAR settings

You can change ALCASAR network settings in the « system » + « network » menu.

a) IP configuration

If you modify the private network IP address, you must restart the devices connected on this network.

⚠️ You can also change these parameters in a text console by editing the file « */usr/local/etc/alcasar.conf* », then by running the program « *alcasar-conf.sh --apply* ».

b) DHCP server

The DHCP (Dynamic Host Control Protocol) server embedded in ALCASAR provides dynamically IP settings to client devices connected on the network.
You must warn this DHCP server if you have devices that use static IP addresses (servers, printers, WiFi Access Point, switches, etc.). This avoids IP conflicts.
Be sure that no other router or DHCP server is connected on your network. Or be sure to well knowing how manage multi-DHCP service (cf. §7.6 to manage the cohabitation with a A.D. © server).

c) Local name resolution

As ALCASAR is is the name server (DNS) on your LAN, you can ask it to resolve the name of your network equipment in order you to connect to them easily. In this example, the server which has the address 192.168.182.5 can be joined directly with its name "my_nas".

2.2.   <u>Users devices settings</u>

a)   Network setting

A "User sheet" is available at the end of this manual.
Users only need a system in **DHCP mode** and a browser supporting **« JavaScript »**. To be intercepted by ALCASAR, browsers must try to access a **HTTP** (not HTTPS) website. You can use for example : http://neverssl.com or http://euronews.com or the welcome page of ALCASAR: http://alcasar.localdomain. The **proxy** settings must be **disabled.**

b)   Adding bookmark

On browsers, it can be useful to add ALCASAR homepage (http://alcasar.localdomain/) to bookmarks in order to allow users to change their password, to log in/out or to install the ALCASAR authority security certificate (see next §).

c)   Installing the ALCASAR security certificate[1]

Some communications between client devices and ALCASAR are encrypted with SSL (Secure Socket Layer) protocol. This protocol needs two certificates created during the installation : the ALCASAR certificate and the local Certification Authority (C.A.) certificate. By default, browsers don't know this certification authority. So, one of the following page is displayed when they communique with ALCASAR for the first time.
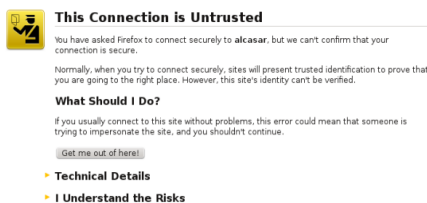
« Mozilla-Firefox »   **« Microsoft-I.E. »**   **« Google-chrome »**

Although it is possible to continue to browse, it is recommended to install the security certificate of this C.A. in browsers so that they don't display these pages anymore. To do that, click the zone « Install ALCASAR AC certificate » of the ALCASAR homepage. For each browser, follow the following steps :

Select « Trust this CA to identify websites ».
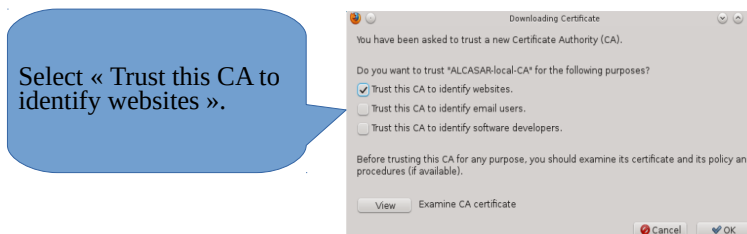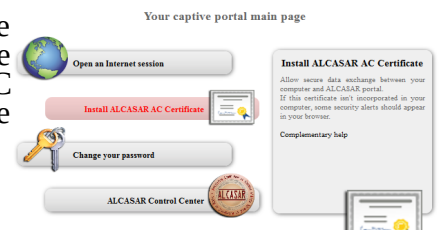
« Mozilla-Firefox »
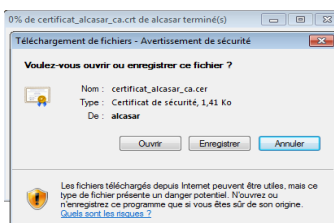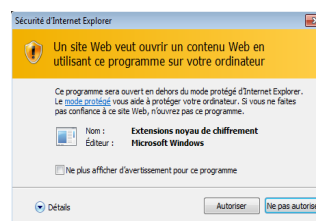
1 – click « open »   2 – click « authorize »   3 – click « install the certificate »   4 – Choose the store « Trusted root certification authorities »
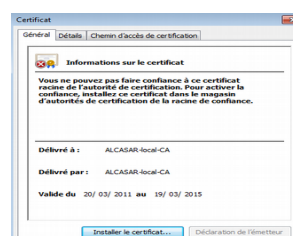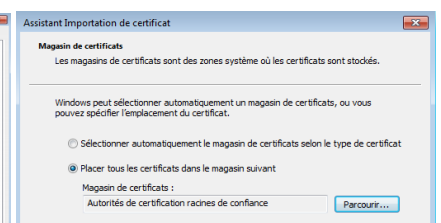
« Internet Explorer 8 » and « Safari »

<u>« Google chrome »</u> : 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 ».

1You can avoid this manipulation either including an official certificate in ALCASAR (see §7.4), or in disabling the encryption of users authenticating flow (ACC: menu "system" then "network" or with the script « alcasar-https.sh {--on|--off} »). Disabling the encryption means that you manage the eavesdropping risk on your consultation network (see §10).

d) Network configuration in static mode (servers, printers, WIFI access points, etc.) :

For these devices, the required parameters are the following :
- default gateway : IP address of ALCASAR on consultation network (192.168.182.1 with default settings) ;
- DNS server : IP address of ALCASAR (192.168.182.1 with default settings) ;
- **DNS suffix : localdomain**
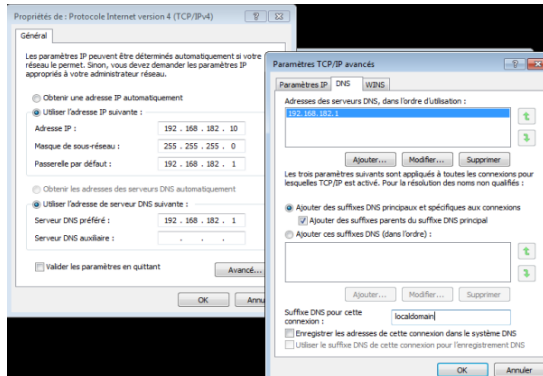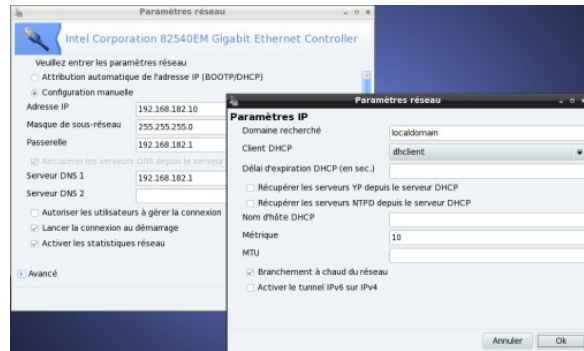
Windows   **Mageia Linux**

e) Time synchronization

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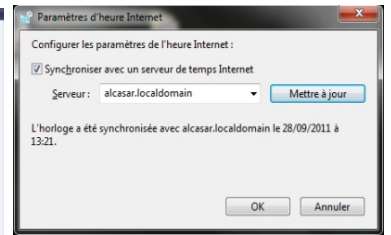
3. Managing users and their devices

User management interface is available in the menu «AUTHENTICATION»).
You can :
- manage the network activity (disconnect a user, authenticate equipment);
- create, search, modify and remove users or user groups;
- import user names from text files or from a backup of the users database;
- empty the user database;
- define trusted web sites that can be joined without authentication (exceptions);
- manage the auto-registration system using GSM adapter and SMS.

3.1. Network activity

A connected user device. You can disconnect it or click on his name to view his profile.

Device allowed permanently to browse the Internet without authentication (trusted device - see §3.8.c)

Device allowed temporarily to browse the Internet.

Device connected on the ALCASAR network but with no user authenticated.
- You can dissociate its IP address (required when tou want to change its IP address and ALCASAR had already recorded the previous one.
- You can authorize it to browse Internet temporarily.

#	IP Adress	MAC Adress	User	Action
1	172.16.5.231	54-EE-75-31-32-FD (Unknown)	rexy (Rexy)	Disconnect
2	172.16.23.56	00-21-CC-D7-BF-B4 (Flextronics International)		Disconnect
3	172.16.1.42	FC-AA-14-25-B7-D1 (Unknown)	@MAC allowed (Calculateur-Paul - 2)	
4	172.16.1.41	FC-AA-14-25-B7-A6 (Unknown)	@MAC allowed (Calculateur-Paul - 1)	
5	172.16.1.43	54-04-A6-04-E5-28 (ASUSTek COMPUTER INC.)	@MAC allowed (AD + TSE)	
6	172.16.1.16	00-11-32-10-EA-5F (Synology Incorporated)	@MAC temporarily allowed	Disconnect
7	172.16.1.31	00-0D-B4-0F-7B-9C (NETASQ)	@MAC allowed (SN150)	
8	172.16.1.10	E8-E7-32-48-FC-EC (Alcatel-Lucent)		Dissociate @IP Temporarily authorize
9	172.16.0.2	00-E0-B6-1A-17-BB (Entrada Networks)	ALCA...stem	
10	172.16.1.30	00-40-8C-EC-D2-27 (AXIS COMMUNICATIONS AB)		
11	172.16.1.20	00-1B-A9-9F-1E-E8 (BROTHER INDUSTRIES, LTD.)		
12	172.16.1.40	00-10-74-A7-04-06 (ATEN INTERNATIONAL CO., LTD.)		

If you see some equipment with IP address "0.0.0.0", that means that this equipment is configured with a static IP address. You should inform ALCASAR of that situation (see §2.1.b).

3.2. Creating groups

Generally, in order to minimize the administration load, it's interesting to manage user group instead of each user. For that, the first thing to do is to define the list of users' group to create.
When you create a user group, you can define attributes of all the users of this group. These attributes are taken into account only if they are not empty. Thus, let the attribute empty if you don't want to use it. For assistance, click on the attribute name.

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)
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
Antivirus & domain Filtering
Network protocols filtering
Status page need to stay open

The name is case sensitive (« group1 » and « Group1 » are two different names) and can't contain any accents or special characters.

Expiry date
After this date, users of this group can't log in anymore. A week after this date, users will be automatically deleted. Click on the zone to see a calendar.

Maximum time of connection
This time of connection is independent of the number of sessions. Thus, the user can spend this time as he wants (in one or more sessions).

3 limit of time
When one of these limits is reached, the user is logged out.

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

Authorized periods in a week
Example for a period from Monday at 7 am to Friday at 6 pm :
Mo-Fr0700-1800
Click on the icon to see a timetable

5 quality of service parameters (QOS)
You can set limitations.
Data volume limit is set for one session. When the limit value is reached, the user is logged out.

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

Antivirus and domain filtering
Choose the filtering policy. See §4 for more explanations about the blacklist, whitelist and antivirus filtering system.

None
WEB Antivirus
Blacklist + WEB antivirus
Whitelist + WEB antivirus

Network protocols filtering
Choose here to filter or not the network protocols.
See §4 to set the customized list of protocols.

None
Web browsing (HTTP & HTTPS)
Web browsing, Mail et remote access
Customized

Status page Needs to stay open
This attribute define whether the user let its "status page" open to stay connected

Filtrage de protocole - Protocol filtering
Cet attribut définit le niveau de filtrage des protocoles réseau pour un usager :
- Aucun : Tous les protocoles réseau sont autorisés
- Navigation Web : Seuls les protocoles HTTP et HTTPS sont autorisés
- Navigation Web, Messagerie et serveur distant : Les protocoles HTTP/S, POP3/S, IMAP/S, FTP, SFTP et SSH sont autorisés
- Personnalisable : La liste des protocoles autorisés est définie dans le menu 'Filtrage' + 'Protocoles'

This attribute defines the protocol filtering level for a user :
- None : All the network protocols are allowed
- Web browsing : Only HTTP and HTTPS are allowed
- Web browsing, Mail et remote server : The protocols HTTP/S, POP3/S, IMAP/S, FTP, SFTP et SSH are allowed
- Custom : the list of allowed network protocols is defined in the menu 'Filtering' +

For assistance, click on the attributes name.

3.3. <u>Editing and removing a group</u>

Click the name of the group to edit it

		Liste des groupes	
#		...upe	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 ? Yes, remove

Groups managment

MEMBERS	ATTRIBUTES	REMOVE

Group : classroom1

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

classroom1
lulu
paulo
sophie

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

Change

Manage the selected user

3.4. <u>Creating users</u>

Login and password are case sensitive
(« James » and « james » are two different users)

If you choose a group, the user inherits its attributes*.

* When an attribute is defined both for user and for his group, user attribute takes precedence over group attribute.
* When a user is a member of several groups, you can set his primary group in the user attributes window (see next §).
* When an attribute prevents a user to log in, a message is displayed in his login window (see « user sheet » at the end of this manual).
* if you set the "surname and name", it will be displayed in the different administrative

Login	
Password	generate
Group	The group list is empty
Surname and name	
Email Address	
Expiration date	
Authorized period after the first connection (in seconds)	s ▼
Number of concurrent login	1
Filtering	None ▼
Voucher language	Français ▼

see the previous chapter to get details on attributes

Create

Or :

Create several tickets

Note: when creating multiple ... ultaneously :
- username and password are ... erated,
- fields "Surname and name" ... ss" are not use.

Advan...d menu

To see/hide all attributes

When the users are created, PDF vouchers are generated in the language of your choice.

TICKET D'ACCÈS INTERNET

ALCASAR

Utilisateur : **Alex**

Mot de passe : **duKbFUo9**

Durée totale autorisée : **1 H**

Durée d'une session : **Illimitée**

Durée journalière : **Illimitée**

Date d'expiration : **04 - 07 - 2012**

Enter the number of users to create

OK   Annuler

If you create multiple users, it's interesting to fix an expiration date (see the remark below)

<u>Remark :</u> if an expiration date is enabled, one week after this date, the user is automatically deleted. When a user is deleted from the database, his connection logs are kept in order to be able to impute his connections.

3.5. <u>Searching and editing users</u>

You can search users with several criteria (login name, attributes, etc.). If you leave the criteria field blank, all users will be listed.

The result is a list of users matching your search criteria. Each user's toolbar includes the following functions :

User attributes

Personal information

Deleting a user

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

Active sessions
(From here, you can disconnect the user)

Connections list
(you can define an observation period)

3.6. Importing users

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

a) From a user database backup

When you import a user database backup, the current database will be emptied. Because this database needs to be provided in case of inquiry, a backup is automatically done (see §7 to retrieve this backup).
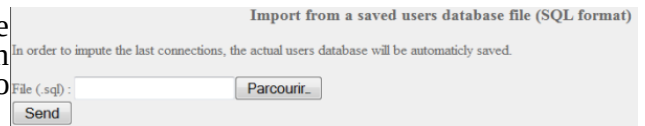
b) From a text file (.txt)

This function allows you to easily add users to the current database. This text file must be formatted like this : one user login per line followed (or not) by a password separated by 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 « Text (DOS) (*.txt) format» ;
- from the « LibreOffice office suite », record the file in « Text CSV (.csv) » format and remove 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 « .txt » and « .pdf » format, including login names and passwords, are created and displayed in ACC for 24 hours. They are saved in the directory « /tmp » of ALCASAR (.pwd extension). These files are removed if you reboot ALCASAR.
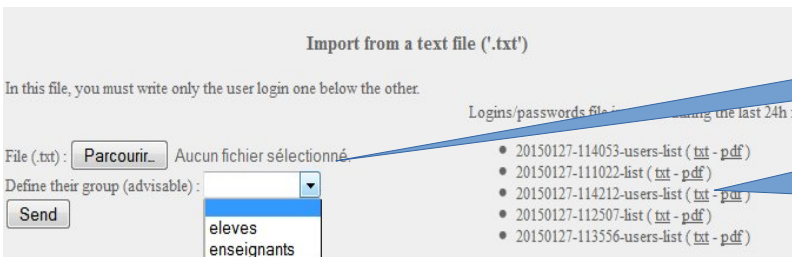
In order to ease the management of new users, you can define their group.

For each import, a file including logins and password is available for 24 hours (« txt » and « pdf » format).

3.7. Emptying the user database

This function allows you to delete all the users in one click. A backup of this database is automatically done. See §7 to retrieve the backup. See previous chapter to re-inject it.
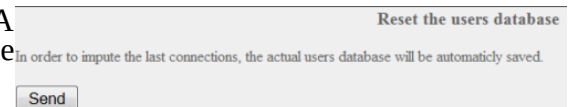
3.8. Authentication exceptions

By default, ALCASAR stop the network flow from equipment where no user is authenticated.
Nevertheless, you can define some exceptions in order to :
- allow auto update of antivirus and auto-update of operating systems (See §11.2) ;
- to access a server or a security zone (DMZ) located behind ALCASAR ;
- to allow some devices to not be intercepted.

a) Trusted sites
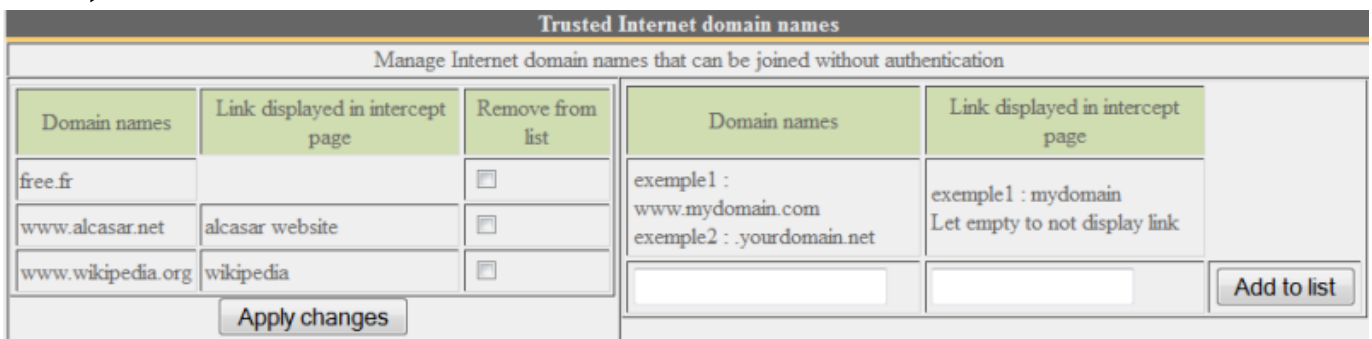
In this window, you can manage trusted site names or trusted domain names. In case of a domain name, all the linked sites are allowed (example : « .free.fr » allows "ftp.free.fr", "www.free.fr", etc.).
You can also decide to display theses sites on the ALCASAR interception page displayed to users.

b) Trusted IP addresses

In this window, you can manage trusted IP addresses or trusted network ip addresses (a DMZ for example). The network protocol filtering, if enabled (see § 4.2.c), has no effect on the addresses mentioned here.

c) Trusted devices

It is possible to allow some devices situated on the consultation network to go through ALCASAR without being intercepted. In order to do that create a user whose name is the MAC address of the device (written like that : "08-00-27-F3-DF-68") and the password is "password". It should be borne in mind that in this case, traces of connection to the Internet will be charged to the device (not to a user).
To display more information than only the MAC address, you can add user information in the "user info" menu (like in the following screenshot).

#	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		eleves
4	jerome_m		eleves
5	laurent_t		eleves

3.9. Auto-registration via SMS

a) Purpose, principle and prerequisite

The objective of this module is to provide to the users a self-registration, while respecting the "french" legal requirements. When we have created this ALCASAR module, we searched for a solution where ALCASAR only receives SMS (no sending) in order to reduce the cost of use.

In order to work, this module required a GSM modem (also called "3G/4G key") with its firmware updated[2], and a basic subscription to a mobile operator.
How does it work? The user who wants an ALCASAR account sends a simple SMS to the number of the ALCASAR GSM modem. The SMS content is the password the user wants to have. When ALCASAR receives the SMS, it creates a new account where the phone number is the login and the text of the SMS is the password of this new account.

During our tests the following GSM modems were used (average cost: 30€) :

- **Ostent with Wavecom Q2303A – USB interface**
  - **recommended modem**
  - Connectivity: USB
  - Connection speed : **9600 bauds**

- **Ostent with Wavecom Q2303A – seriel-rs232 interface**
  - Connectivity: RS-232 (with an RS-232/USB link)
  - Power: extern with 220v adapter
  - Connection speed : **115200 bauds**

- **Huawei E220**
  - Connectivity: USB
  - Remark : minimal firmware version: 11.313.02.00.01
    - cf. https://www.geeek.org/huawei-e220-firmware-update-windows-10-072.html.
  - Connection speed : **115200 bauds**

- **We detect some issues with that following modems :**
  - **Huawei E180** (the communication port randomly changes).

---

2   Cf : https://www.modemunlock.com

b) Enable the service

You can have access to the configuration of this module in the autoregistration entry.

If no 3g key are plugged, the configuration page is disabled.

Status of your device

No device detected

⚠ If a valid 3g key is connected (**don't start the service before entering all the information !!!**) :

Auto registration (SMS)

☑ Refresh : 30 sec

Status of your GSM MODEM (2G/3G/4G key)

A GSM MODEM 'HUAWEI_Mobile(E220 HSDPA Modem / E230/E270/E870 HSDPA/HSUPA Modem)' is connected.
It has openned the following ports : /dev/ttyUSB0 /dev/ttyUSB1

Configuration			Current configuration
Connection port to the MODEM	/dev/ttyUSB0 ⌄	Modify	/dev/ttyUSB0
Connection speed to the MODEM	115200 Bauds ⌄	Modify	115200 Bauds
Phone number of the SIM card		Modify	+33652491042
PIN password of the SIM card		Modify	1234
Validity period of new account	days Modify		1
Max number of try before a permanent ban		Modify	3
Duration of a ban (for example, after X try)	days Modify		2

Service status		Signal strength	Device IMEI	Number of SMS received
❌ The service is down	Start Stop	-	-	-

Port number and connexion speed[1]

Phone number of the 3g key[2]

PIN code to unlock the SIM card Be sure !!![3]

Time available when an account is created[4]

Number of try before a ban & time of a ban[5]

Beware that the configuration is correct before starting the service

[1] Each 3g key has a different baud rate transfers. See previous chapter to find the rate for the 3g keys we have tested. If you use another model, a bigger list of configuration can be found on : http://wammu.eu/phones/
[2] This number must be written as the international pattern: +xxYYYYYYYYY. « xx » for country indicative. « YYYYYYYYY » for the phone number (9 digits). This number will be written on the user information page (see next §). Example : for the French number "0612345678", the international number is "+33612345678".
[3] Be careful, if the PIN code is wrong, the SIM card will be locked. In this case, follow the instructions in the technical documentation of ALCASAR (§8.2 Auto-inscription par SMS) to unlock it.
[4] This field gives a value (in days) for a valid account.
[5] A policy against the spam has been implanted :
   • Number of tries allowed by phone when receiving an invalid password (just one word in the content of the SMS).
   • If the number of tries is exceeded, the phone number of this user will be banned for a time (in days). Each phone number ban will be ignored by ALCASAR.

If all is set correctly, you can start the module with the "start" button. Then, wait for about 30'. When the service is started, wait again for the key (recording process on the GSM infrastructure). If all is ok, the service display the following status:

Service status			Signal strength	Device IMEI	Number of SMS received
✓ Gammu is running	Start	Stop	▂▃▅ -- 60 %	353805013215525	0

This table shows the status of the service, the signal strength, the IMEI number and the number of SMS received (reset when the service is restarted).

c) User interface

Once the service is started, the interception page provides an additional link « Auto registration ». The ALCASAR main page also displays a dedicated link (http://alcasar.localdomain).

This link gives some information about the SMS account already created. Moreover, each user can have some information on the status of his phone number.

d) Accounts management [administration]

Each account created by the auto-registration module has just one attribute : the expiration date. These accounts belong to the users group "sms". So, if you want to set an attribute, you can edit the "sms" user group (see §3.2). These accounts are not seen in the standard user management section of the ACC.

This table gives the state of phone number which have sent one or more SMS. If you click on delete, the account (if it is already available) will be deleted, and the user can create an account again.

e) Country filtering

By default, the SMS auto registration module allows only French numbers (country code: +33). A web interface is available to change the level of filtering:
- only French numbers
- only European numbers
- Allow every numbers
- Personal configuration: the administrator can authorize a personal list of countries.

f) Error messages [administration]

Cannot listen the ttyUSB0 port.	You GSM modem is probably used by another program.
Timeout. Cannot connect to the GSM modem.	The GSM modem has been disconnected.
An issue with your Sim card was detected. Is it in the key?	The Sim card is not in the GSM modem.
Warning, during the last startup, the PIN code was wrong.The Sim card must be blocked. Please read the documentation.	The PIN password is invalid. The SIM card is maybe blocked. Please instructions in the technical documentation of ALCASAR (§8.2 - Auto-inscription par SMS ».

4. __Filtering__

FILTERING
▸Blacklist
▸Whitelist
▸Protocols

ALCASAR has several optional filters:
- a blacklist and a whitelist of domain names, URLs and IP addresses;
- an anti-malware on the WEB flow;
- a filter for network protocols.

The first filter was developed at the request of organization likely to welcome young people (schools, secondary schools, recreation centers, etc.). This filter can be compared to the parental/school control system. You can enable or disable it for each user (or group of users) by modifying users or groups attributes (see §3).

Domain names, URLs and IP addresses are referenced in two lists.
- Either you operate a whitelist. The filtered users using that list can access only the sites and IP addresses of the whitelist
- either you operate a blacklist. The filtered users using that list can access all the sites and IP addresses except those of the blacklist.

| Filtering | := ▾ | None ▾ |
| None |
| Antivirus |
| Blacklist + antivirus |
| Whitelist + antivirus |

On ALCASAR, this filter runs on all network protocols. For example, if the domain name "warez.com" is blocked, all protocols for this domain will be blocked (HTTP, HTTPS, FTP, etc.).

ALCASAR uses **the excellent** list (black + white) drawn up by the University of Toulouse (France). This list was chosen because it is distributed under a free license (creative commons) and its content refers to France. In that list, domain names (eg www.domaine.org), URLs (eg www.domaine.org/rubrique1/page2.html) and IP addresses (eg 67.251.111.10) are listed by categories (games, astrology, violence, sects, etc.). The ACC allows you :
- to update that list and to define the categories of sites to block or to allow;
- to rehabilitate a blocked site (exemple : a site that was banned, was closed and purchased by new people);
- to add sites, URLs or IP addresses that are not in the list (CERT alerts, local directive, etc.).

This filtering system can be enabled by user (or by users group). When enabled, it is linked with an anti-malware that can detect a lot of type of files (virus, worm, phishing, etc.) which is updated every 4 hours.

4.1. __Blacklist and Whitelist__

a) __Updating the list__

To update the lists, download the latest version of the list of the University of Toulouse (France) and install it. Once the file is downloaded, ALCASAR calculates and displays its fingerprint. Then, you can compare this fingerprint with the one available on the website of the University of Toulouse. If the two are identical, you can confirm the update. Otherwise, discard it.

List version : January 05 2013

[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 (line 'blacklists.tar.gz') : dsi.ut-capitole.fr/blacklists/download/MD5SUM.LST

[Activate the new version] (Estimated time : one minute.)

[Reject]

b) __Editing the blacklist__

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

redirector

Some redirector sites, which are used to circumvent filtering.

Number of filtered domain names : 84482
Number of filtered URL : 291
Number of filtered IP : 250

BlackList

Domain names : 1248186, Url : 54296, Ip : 214557
Select the categories to filter

arjel ☐	astrology ☐	audio-video ☐	blog ☐	celebrity ☐	chat ☐	cooking ☐	filehosting ☐	financial ☐	forums ☐
games ☐	lingerie ☐	manga ☐	mobile-phone ☐	publicite ☐	radio ☐	reaffected ☐	shopping ☐	social_networks ☐	sports ☐
webmail ☐	adult ☑	agressif ☑	dangerous_material ☑	dating ☑	drogue ☑	gambling ☑	hacking ☑	malware ☑	marketingware ☑
mixed_adult ☑	phishing ☑	redirector ☑	remote_control ☑	sect ☑	strict_redirector ☑	strong_redirector ☑	tricheur ☑	warez ☑	

Example(s) :

100md.com/proxy
1337games.net/proxy/
207.156.166.165/anonymiser
208.53.147.202/~regvinfo/
24web.mobi/proxy
64.27.4.141/?pagename=www
66.197.221.187/~unlockwe/
66.90.103.130/~bypassww
74.86.47.189/~hidemypr/
94.23.46.192/filesonic-proxy.php
acewebmedia.com/myspaceproxy
adguru.org/proxy
alltooflat.com/geeky/elgoog
america22.net23.net/index.html/
andrewtchin.com/proxy/

[Close]

By clicking on the category name, you display its definition and the number of domain names, URLs and IP addresses it contains. By clicking on one of these number, you display the first 10 values.

You can rehabilitate domain names or IP addresses.

You can add domain names or IP addresses directly in the ACC or by importing text files. These files can be enabled, disabled or removed. Each line of these test files can be a domain name or an IP address.

As an example, ALCASAR team brings a first file with all the access nodes of the TOR network. This forbid access to this anonymous network.

<u>Info</u>: if you want to test site filtering or site restoring, remember to clear the cache memory of the browsers.

c) Special blacklist filtering

The blacklist has two special filters available for HTTP protocol. The first one blocks URLs containing an IP address instead of a domain name.

The second one exclude results from Google search engines that may not be suitable for minors ("Safe search" function).

It works with "YouTube" only if you get a YouTube ID. For that, visit : http://www.youtube.com/education_signup. Once your YouTube account is created, copy the ID in the ACC and save the changes.

Once your account is created, get your Youtube ID (character string just after the ':' character).

d) Editing the Whitelist

As for the blacklist, you can select categories and add your own domain names and IP addresses.

Note : "liste_bu" is a category used by French students (bu=bibliothèque universitaire=university library). This category contains a lot of useful websites validated by teachers and learning teams.

4.2. Customized protocols filtering

If you have enabled the network protocols filter named "customized" (see. §3.2 & §3.4), it's here you can define the list of protocols you authorize. A list of standard protocols is presented by default. You can enrich it.

- ICMP is used for example by the «ping» command.
- SSH (Secure SHell) : to allow secure remote connections.
- SMTP (Simple Mail Transport Protocol) : to allow emails to be sent from a thick client (Outlook, Thunderbird, etc.).
- POP (Post Office Protocol) : to allow thick clients to download emails.
- HTTPS (HTTP secure) : to allow secure web surfing.

5. Access to Statistics

STATISTICS
- user/day
- connections
- daily use
- global trafic
- detailed trafic
- security

Statistics are available on the ACC (menu "statistics"), after logging in.
This menu 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);
- global & detailed network traffic (updated every 5 minutes);
- security reports (updated in real time).

5.1. Number of connections per user per day

This page displays, per day per user, number, connection time and volumes of data exchanged.
Please note: 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

One line per day

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

You can customize this state by:
- Filtering on a particular user;
- Defining a certain period of time;
- Sorting with different criteria.

start time: 2007-05-30   stop time: 2007-06-06   pagesize: 10   sort by: connections number   order: ascending   [show]
On Access Server: all   User:

5.2. Connection status of users

This page lists login and logout events from the portal. An input box allows you to specify your search and display criteria.
With no search criteria, the chronological list of connections is displayed (since the installation of the portal).
Please note: 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

Critère de sélection :
--Attribute--

Classé par :
Accounting Id

Nbr. Max. de résultats retournés
40

[Envoyer]

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

Select 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 search are detailed below.

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

Journal des connexions

Afficher les attributs suivants :
Accounting Stop Delay
AcctAuthentic
CalledStationId
Caller Id
Client IP Address

Critère de sélection :
--Attribute--
Login Time   >=   2009-06-01   [del]
Login Time   <=   2009-06-15   [del]

Classé par :
Accounting Id

Nbr. Max. de résultats retournés :
40

[Envoyer]

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	393.42 KBs	2009-06-04 16:57:39	2009-06-04 18:25:17	1 hours, 27 minutes, 38 seconds	5.57 MBs	

- Examples of search No2 : Display of the 5 shortest connections during the month of July 2009 and with the IP address "192.168.182.129". The display criteria include the cause of disconnection but not 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	

5.3. Daily use

This page allows you to know the daily load of the portal.
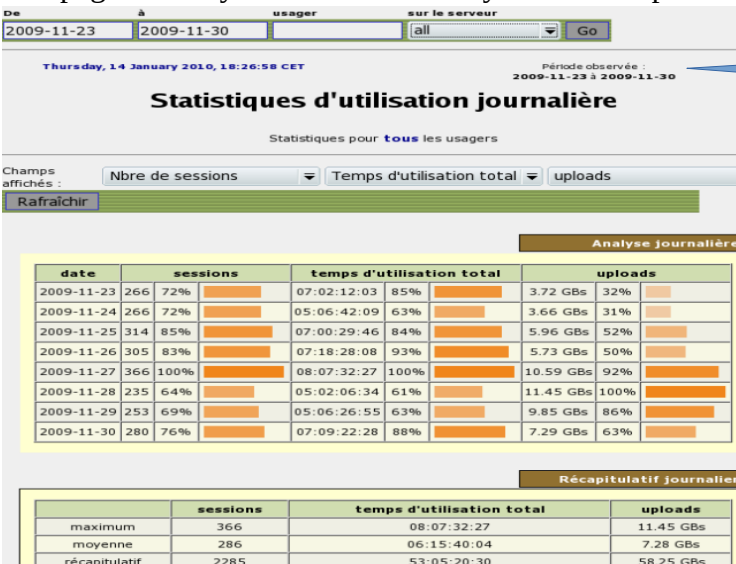
Here, set in the period. You can specify a particular user (leave this field blank to accommodate all users).

5.4. Global and detailed traffic

Global traffic
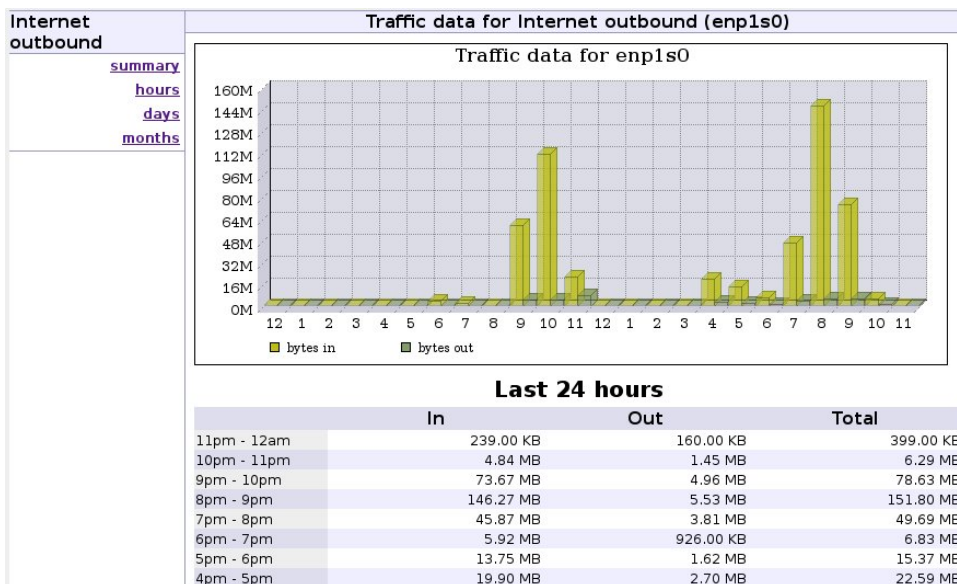
This graph allows to show network statistics by the hour, day, month.

Detailed traffic

This page shows the statistics for outbound network traffic (by day, by the week and by the month). The data are updated every 5'.
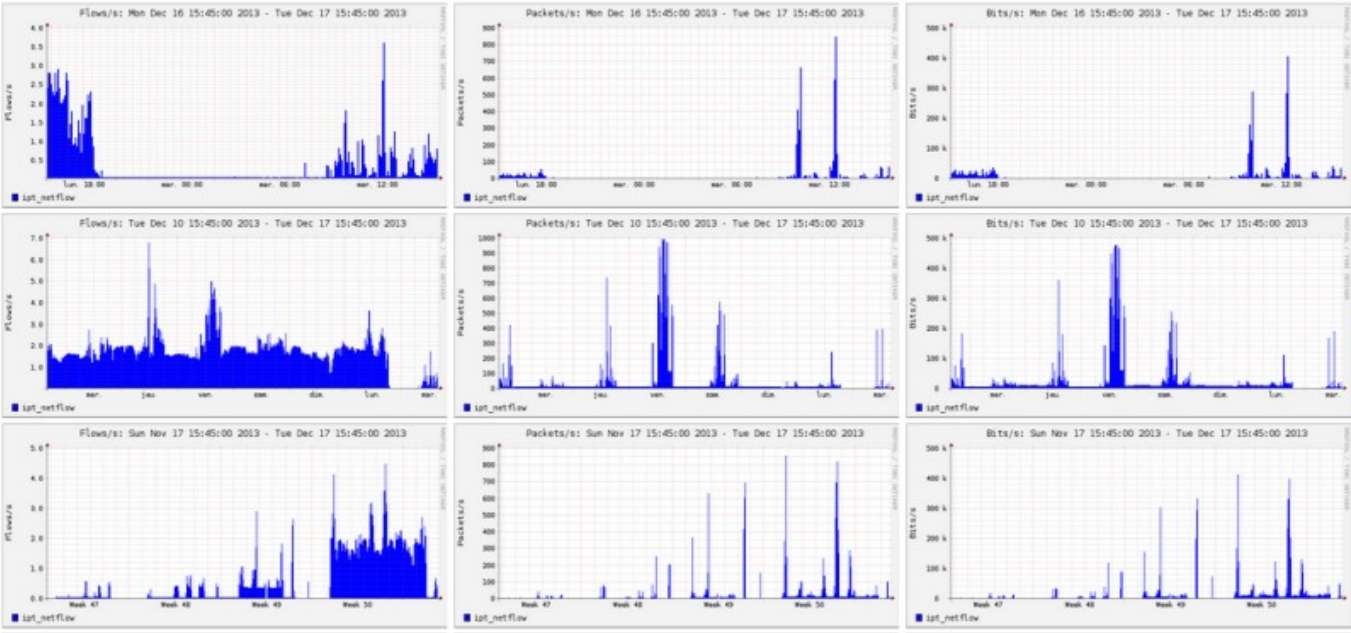
The "details" menu allows you to zoom on a particular time slot. For the HTTP flows, network IP addresses are hidden and replaced with the IP address of ALCASAR.

The "plugins" menu shows the network traffic based on the traffic protocol (port tracker). You can see the protocols currently in use ("now") or all protocols used during the last "24 hours".

SURFmap is a plugin which gives the possibility to have a visual of all the flows (not only HTTP). Your web-browser must be connected to Internet to retrieve the base map!!!

Different filters are available in the *Menu* : number of flow, begin and end date, show just the flows of one @ip ("src host 123.123.123.123")
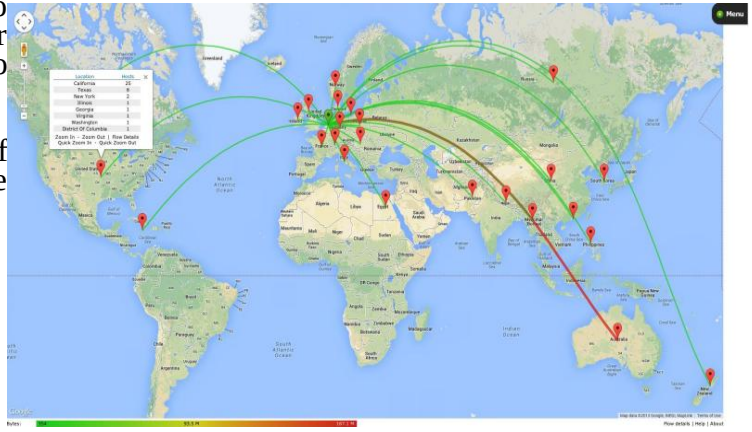
Do not enter a huge value of flow. More this value is high, more the time of process is high.

The "*Auto-refresh*" *checkbox* refresh this page each 5 minutes.

5.5. Security Report

This page displays three safety information identified by ALCASAR:
- The list of users disconnected due to a MAC address spoofing of their device;
- 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 SSH connection failures – 5 successive connection failures on the ACC – 5 successive login failures for a user – 5 successive attempts to change password in less than one minute.

Adresse(s) MAC usurpée(s) (Watchdog)

alcasar-watchdog : 172.16.0.10 is usurped (54-04-A6-1E-F7-DB). Alcasar disconnect the user (
alcasar-watchdog : 172.16.0.10 is usurped (54-04-A6-1E-F7-DB). Alcasar disconnect the user (
alcasar-watchdog : 172.16.0.10 is usurped (54-04-A6-1E-F7-DB). Alcasar disconnect the user (
alcasar-watchdog : 172.16.0.10 is usurped (54-04-A6-1E-F7-DB). Alcasar disconnect the user (
alcasar-watchdog : 172.16.0.10 is usurped (54-04-A6-1E-F7-DB). Alcasar disconnect the user (
alcasar-watchdog : 172.16.0.10 is usurped (54-04-A6-1E-F7-DB). Alcasar disconnect the user (
alcasar-watchdog : 172.16.0.10 is usurped (54-04-A6-1E-F7-DB). Alcasar disconnect the user (
alcasar-watchdog : 172.16.0.10 is usurped (00-24-81-12-52-01). Alcasar disconnect the user (

Virus bloqué(s) (HAVP)

2013 Aug 30 18:16:55 127.0.0.1 GET 200 http://securite-informatique.info/virus/eicar/download/eicar_niveau1.zip 276+474 VIRUS ClamAV: Eicar-Test-Signature
2013 Oct 03 10:15:29 127.0.0.1 GET 200 http://am4-r1f9-stor05.uploaded.net/dl/efb34de0-af7b-4851-81d0-caa42ca4a2e4 299+5000632 VIRUS ClamAV: Win.Trojan.Agent-108073
2013 Oct 03 11:30:49 127.0.0.1 GET 200 http://www.hackerzvoice.net/ceh/CEHv6%20Module%2008%20Trojans%20and%20Backdoors/valvnet20b2.zip 298+1484772 VIRUS ClamAV: Trojan.Netbus.KeyHook170
2013 Oct 03 11:31:39 127.0.0.1 GET 200 http://www.hackerzvoice.net/ceh/CEHv6%20Module%2008%20Trojans%20and%20Backdoors/Nuclear%20RAT%20Trojan/client.exe 308+852 ClamAV: Trojan.Dropper.Delf-152
2013 Oct 03 11:42:33 127.0.0.1 GET 200 http://www.drivehq.com/folder/p7275651/1833479246.aspx 471+182652 VIRUS ClamAV: PHP.C99-5
2013 Oct 07 16:07:52 127.0.0.1 GET 200 http://b   305+5001325 VIRUS ClamAV: PHP.Optix
2013 Oct 07 16:09:53 127.0.0.1 GET 200 http://b   305+5001085 VIRUS ClamAV: PHP.Optix

Adresse(s) IP bloquée(s) (Fail2Ban)

2013-09-25 11:52:51,640 fail2ban.actions: WARNING [ssh-iptables] Ban 172.16.0.12
---> 2013-09-25 12:02:52,370 fail2ban.actions: WARNING [ssh-iptables] Unban 172.16.0.12
iptables -D fail2ban-SSH -s 172.16.0.12 -j ULOG --ulog-prefix "Fail2Ban -- DROP" returned 100

6. <u>Backup</u>

6.1. <u>Connection logs</u>

Traceability log files

- traceability-20150720-05h35.tar.gz (1.9 Mo)
- traceability-20150713-05h35.tar.gz (364.95 Ko)
- traceability-20150706-05h35.tar.gz (1.39 Mo)
- traceability-20150629-05h35.tar.gz (1.55 Mo)
- traceability-20150622-05h35.tar.gz (1.58 Mo)
- traceability-20150615-05h35.tar.gz (1.18 Mo)
- traceability-20150608-05h35.tar.gz (1.19 Mo)
- traceability-20150601-05h35.tar.gz (2.56 Mo)
- traceability-20150525-05h35.tar.gz (1.76 Mo)

The first column displays the list of traceability files containing the users activity logs. To save them on another media "right click" on the file name, then "save target as".

These files are automatically generated once a week in the directory « */var/Save/archive/* ». The files older than one year are deleted.

You can create the traceability log file for the current week.

`Create the traceability file of the current week ⌄` `Execute`

6.2. <u>The users database</u>

Users database

- alcasar-users-database-20150726-11h18.sql.gz (255.27 Ko)
- alcasar-users-database-20150310-21h41.sql.gz (189.65 Ko)
- alcasar-users-database-20150310-00h11.sql.gz (1.75 Ko)

The second column displays backup files (in compressed "SQL" format) of the users database. They can be generated at any time by clicking in the menu "Create the current users database file".

These files can be imported in ALCASAR (cf. §3.6.a). You can use these files when reinstallation of the portal (see §8.4).

`Create the current users database file ⌄` `Execute`

6.3. <u>Weekly activity reports</u>

Weekly activity reports

- alcasar-report-2017-03-19.pdf (39.15 Ko)
- alcasar-report-2017-03-18.pdf (39.18 Ko)

The third colomn displays the weekly activity reports. They are created every monday morning (only in French at the moment – translation in progress…).

6.4. <u>Accountability logs</u>

In case of legal inquiry, law enforcement officials may ask for connection logs of your users. You can generate an accounting logs file of all the users for a specific period. This file will be cyphered (AES256). To see this file, use "7-zip" program under Windows (p7zip under Linux).

⚠ To prevent abuses, all the ALCASAR users will be warned at their next connexion.

⚠ The creation of this log file can take **a very long time** (more than 5'). Be patient and don't change the ACC page.

Extraction des journaux à partir du 2017-03-22 07:00:00

Date de création 2017-03-22

Username	Client @MAC	Client @IP	Login Time	Logout Time	Upload	Download	Cause
███████	8C-84-07-11-31-87	192.168.182.44	2017-03-22 07:03:03	2017-03-22 12:41:15	1939942	57103945	Lost-Carrier

N°	@IP src	Port src	@IP dst	Port dst	Date
1.	192.168.182.44	43903	216.58.198.195	80	2017-03-22 07:03:08.560
2.	192.168.182.44	47263	216.58.198.206	443	2017-03-22 07:03:08.780
3.	192.168.182.44	60930	216.58.198.206	443	2017-03-22 07:03:08.980
4.	192.168.182.44	48603	216.58.198.206	443	2017-03-22 07:03:09.130
5.	192.168.182.44	51378	64.233.166.188	5228	2017-03-22 07:03:09.210
6.	192.168.182.44	54766	54.235.132.180	443	2017-03-22 07:03:11.150
7.	192.168.182.44	34810	179.60.192.3	443	2017-03-22 07:03:11.200
8.	192.168.182.44	38503	179.60.192.3	443	2017-03-22 07:03:11.500

7. <u>Advanced features</u>

7.1. <u>Administrator accounts management</u>

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 to control the operating system ;
- « sysadmin » : This account allows you to take secure remote control of your system (see next §).

Along with these two "system" accounts, "ALCASAR administrator" accounts have been defined to control some functions through the graphical ALCASAR Control Center (ACC). These "administrator" accounts can belong to one of the three following profiles:
- « admin » : with this profile, the accounts give access to all the functions of the ACC. A first "admin" account was created during the installation of ALCASAR (see Installation documentation);
- « manager »: with this profile, the accounts only gives access to users and groups management functions (see §3) ;
- « backup » : with this profile, the accounts only gives access to backup and archiving of log files (see previous chapter).

You can create as many administrator 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

7.2. <u>Secure administration across the Internet</u>

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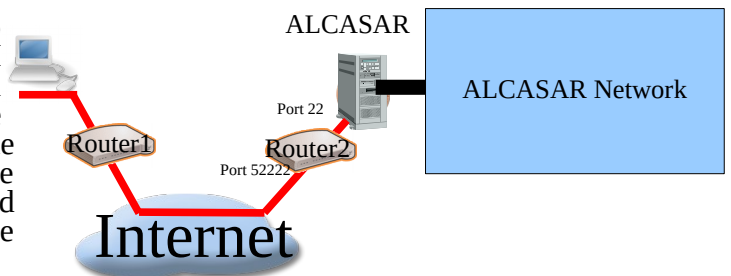
a) Broadband modem/router configuration

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). If you want, you can still use the port 22.
Refer to your broadband modem/router documentation before performing this operation.

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 § 11.1). Use the "su" command to become "root".

- On Linux, install "openssh-client" (you can also install "putty") and run the command « *ssh -p 52222 sysadmin@w.x.y.z* » (replace « w.x.y.z » with the public IP address of the broadband modem/router#2 and replace the "external_port" with the listening port number of the broadband modem/router#2 (52222 in our example). You can add the "-C" option to enable the compression algorithms.
- On Windows, install "Putty" or "putty-portable" or "kitty" and create a new session:
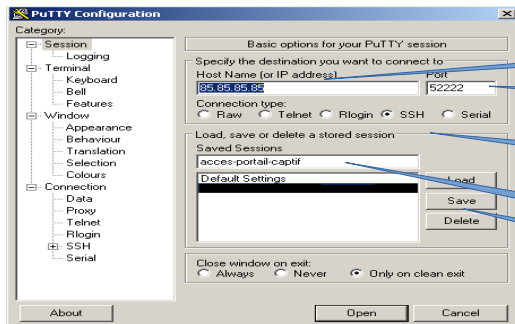
Public IP address of the broadband modem/router#2

Listening port for the administration in ssh mode

Protocol

Session name

Save the session before finish

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

c) Administration ALCASAR in GUI mode

The goal is now to redirect the data flow from the workstation browser, through the SSH tunnel, to the internal network card of ALCASAR. To create this tunnel:

- On Linux, run the command:
  « *ssh -L 10000:@IP_alcasar_internal_card:443 -p 52222 sysadmin@w.x.y.z* »
- On Window, configure « putty » as describe below:

  - 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 internal network card of alcasar followed by the port 443 (here 192.168.182.1:443)
  - 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
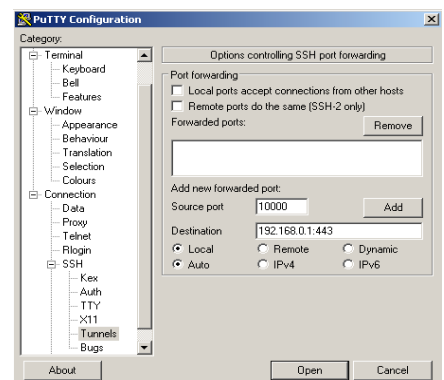
Start your browser and go to : "https://localhost :10000/acc/"
⚠ ("acc/" in the end of URL is important!)
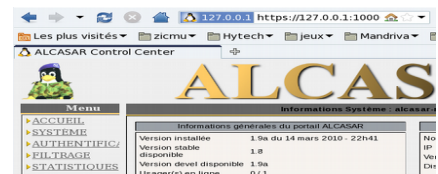
d) Managing devices on the ALCASAR network

Following the same logic, it is possible to manage any device connected to 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_quipment » is the IP address of the device to manage. « NUM_PORT » is the administration port of this equipment (22, 80, 443, etc.).
- On Windows, enter the IP address and the port of the device in the form "Destination" of "Putty".

Run the command : *« ssh login@localhost:10000 »* to use SSH for secure remote administration.
To connect the web-based interface, go to : *« http(s)://localhost :10000 ».*

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

This paragraph, although not essential, adds an additional layer of security using private key authentication.
- generate a keys pair (public key / private key)
  - On Windows with « puttygen »

- open "PuttyGen"
- check the "SSH-2 RSA" box
- specify a key length of 2048 bits
- click on "generate"
- move the mouse to generate random values.

The keys are now created.
- *Enter a representative comment in the "Key-comment" field;*
- *Enter and confirm the passphrase in the "Key passphrase" field;*
- *Save private key by clicking on "Save private key";*
- *Select and copy the public key (right click)*
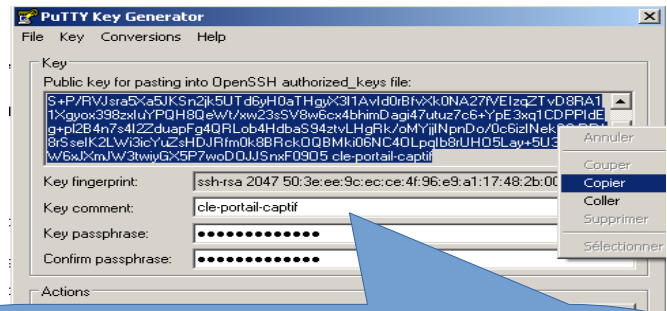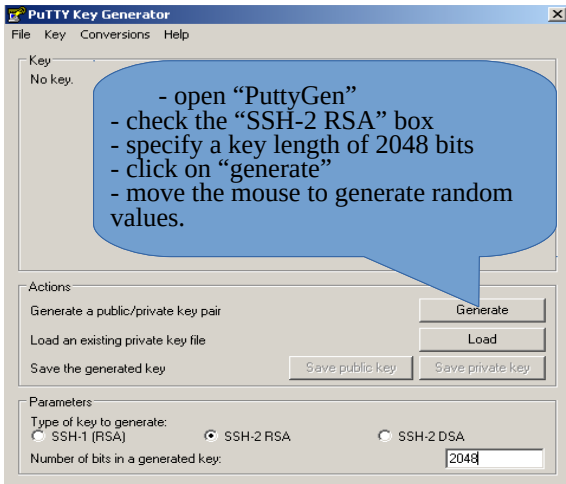
  - Linux with« *ssh-keygen* »

In your personal directory, create the directory « *.ssh* » if it does 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* » displays your public key and allows you to copy it.

```
[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.
```

```
[          .ssh]$ cat id_rsa.pub
ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAQEAyL4yMM8BO18Quusv1Iq/W
3kF2wvhuHzmNmH9ITFTALwHPHA9lWnxlcDPE9DPR7FPqrEZf/uT84C2G1
o7d/IX+/JyPlVXoUdXaZ9wjtusU3SVWSr6o9NXmbZqoOgzrGpjN7Vfu53
npCrDQGfuq6PIm06AQCJQkySmOXDIGFVr4r5Zbw==
```

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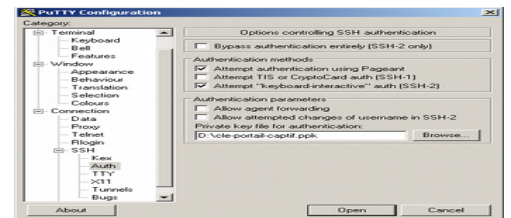
```
[          ]$ slogin sysadmin@
Bienvenue sur alcasar-rexy-74
Enter passphrase for key '/home/richard/.ssh/id_rsa':
Last login: Sat Apr  3 20:14:51 2010 from
alcasar-rexy-74:~$ 
```

7.3. Display your logo

It is possible to display your logo by clicking on the logo on the upper right corner of the ACC. 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. Refresh the page to see the change.

7.4. <u>Modifying the certificate of security</u>

Data is encrypted between ALCASAR and devices on the ALCASAR network in the following cases :
- for users : authentication request and changing passwords;
- for administrators : access to the 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 the homepage of the ACC. If the server certificate is expired, you can regenerate it with the following command : « *alcasar-CA.sh* ».

Système	
Nom d'hôte cannonique	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 using the new one.

a) Installation of an official certificate

It is possible to install an official certificate instead of the auto-signed certificate. The installation of such certificate avoids security warnings on browsers that did not install the certificate of the certification authority of ALCASAR (cf. §2.2.c).
To acquire your certificate, follow the instructions of your provider knowing that the Web server used in ALCASAR is an "Apache server with mod SSL".
Tips: You must have a domain name (ex: mydomain.org). Then, create a certificate for the server "alcasar.mydomain.org". Via the ACC, you can import this certificate (menu : "System" +"Network"). The files you need are:
- The private key you used to create the "certificate request" (extension : .key)
- The certificate created by the provider (extension : .crt)
- Optionally : the file which defines the certification chain of your provider (extension : .crt). When requested, this file is available on the provider website.

Example with the provider "Gandi.net", the domain name "rexy.fr" and a certificate for a server named "alcasar.rexy.fr" :

Once imported, you must reboot all the devices connected to the consultation network (the same thing for your computer).

Certificate import

Private key (.key) : [Parcourir...] alcasar.rexy.fr.key
Certificate (.crt) : [Parcourir...] alcasar.rexy.fr-certificate-247730.crt
Server-chain (if necessary : .crt) : [Parcourir...] GandiStandardSSLCA2.crt
[Import]

Current certificate

Expiration Date : Jul 23 21:03:05 2019 GMT
Common name : alcasar.localdomain
Organization : ALCASAR-Team

Validated by :

Common name : ALCASAR-local-CA
Organization : ALCASAR-Team

[Back to default certificate]

⚠ In case of issues, you can go back to the original auto-signed certificate via ACC or with the command line : « alcasar-importcert.sh -d ».

b) Installation of an official certificate from « Let's Encrypt »

In order to use a free and official certificate, you can use the Certificate Authority (C.A.) "Let's Encrypt". This Authority provides automatic certificates importation procedures. These procedures have been embedded in ALCASAR via the « *alcasar-letsencrypt.sh* » script. Before running these procedures, you must have a domain name. You must be able to add/remove DNS records for that domain name. To ask for a « Let's Encrypt » certificate, you must proof that you are the owner of the domain name. For that, « Let's Encrypt » challenge you with several ways. As ALCASAR can't be contacted directly from the Internet, we use the « DNS-01 » challenge which operates as follows :
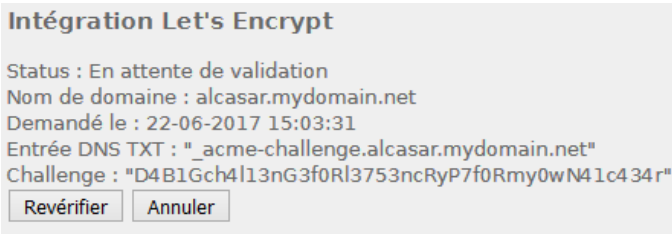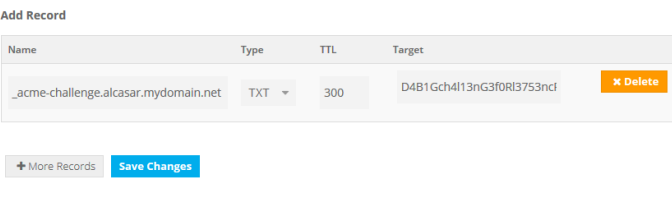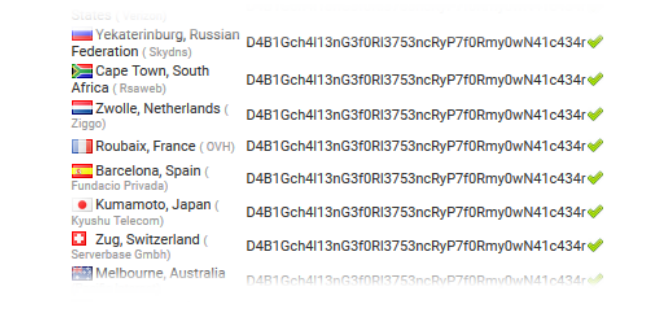
When you ask for a certificate, "Let's Encrypt" send you strings which must be retrievable when asking your domain name (the challenge). Then, you must create a "TXT" DNS entry in your DNS zone with this string. After that, you have to ask "Let's Encrypt" to verify it. Once validated, you can use your certificate. The following scheme shows you the automatic certificate creation process.
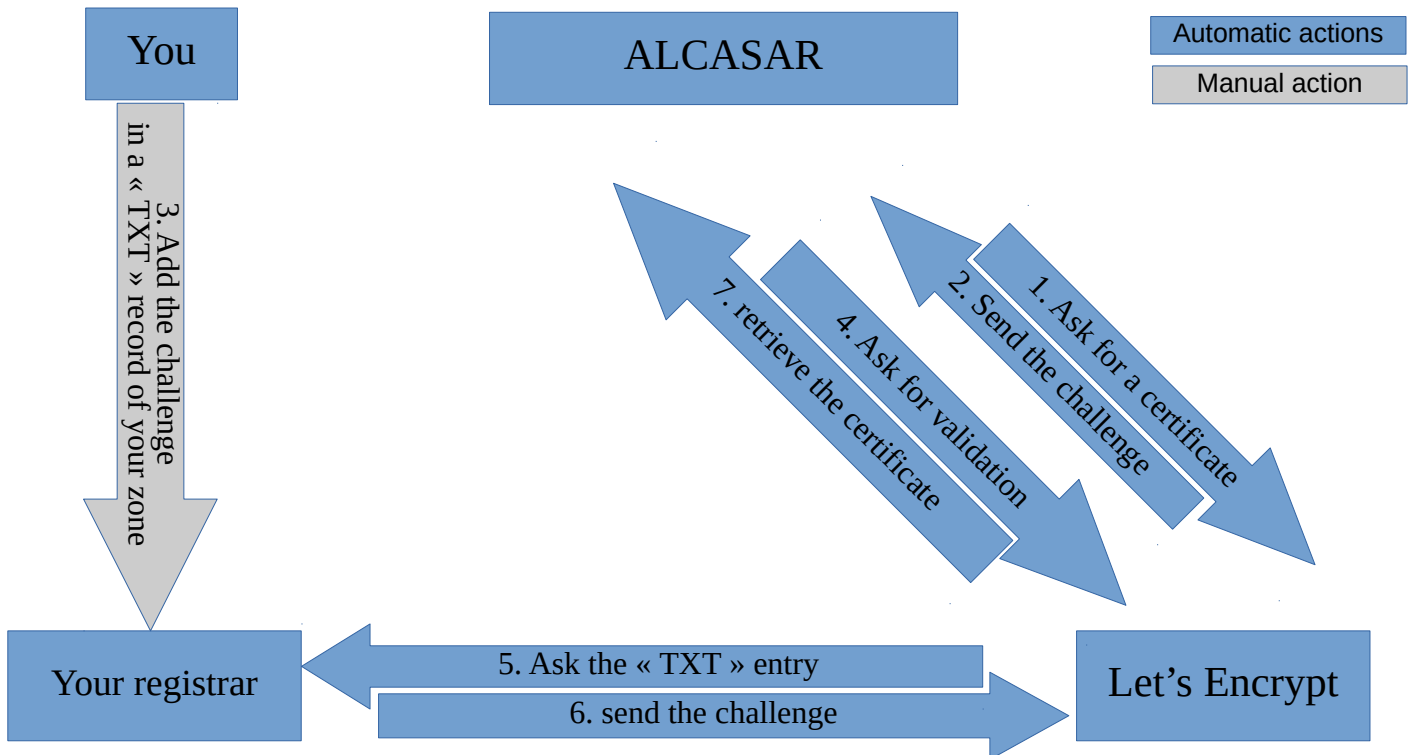
On ALCASAR, you can run the automatic certificate creation process in two ways : via the ACC or with in command line.

Via ALCASAR Control Center (ACC)

Messages displayed on ACC	Actions
	Write your email address. Write the domain name of your ALCASAR (hostname with domain name).

Messages displayed on ACC	Actions
Intégration Let's Encrypt Status : En attente de validation Nom de domaine : alcasar.mydomain.net Demandé le : 22-06-2017 15:03:31 Entrée DNS TXT : "_acme-challenge.alcasar.mydomain.net" Challenge : "D4B1Gch4l13nG3f0Rl3753ncRyP7f0Rmy0wN41c434r" [Revérifier] [Annuler]	A file containing the challenge is sent by "Let's Encrypt". It is displayed in the ACC. It is also saved on ALCASAR in the file "/usr/local/etc/alcasar-letsencrypt".
Add Record Name — Type — TTL — Target _acme-challenge.alcasar.mydomain.net — TXT — 300 — D4B1Gch4l13nG3f0Rl3753ncl — [✕ Delete] [+ More Records] [Save Changes]	On the Web site of your registrar, modify your DNS zone, adding a new TXT record named "_acme-challenge..." which the value is the challenge (see previous step). Note : choose a low TTL in order to speed up the propagation process through DNS servers.
Yekaterinburg, Russian Federation (Skydns) — D4B1Gch4l13nG3f0Rl3753ncRyP7f0Rmy0wN41c434r ✔ Cape Town, South Africa (Rsaweb) — D4B1Gch4l13nG3f0Rl3753ncRyP7f0Rmy0wN41c434r ✔ Zwolle, Netherlands (Ziggo) — D4B1Gch4l13nG3f0Rl3753ncRyP7f0Rmy0wN41c434r ✔ Roubaix, France (OVH) — D4B1Gch4l13nG3f0Rl3753ncRyP7f0Rmy0wN41c434r ✔ Barcelona, Spain (Fundacio Privada) — D4B1Gch4l13nG3f0Rl3753ncRyP7f0Rmy0wN41c434r ✔ Kumamoto, Japan (Kyushu Telecom) — D4B1Gch4l13nG3f0Rl3753ncRyP7f0Rmy0wN41c434r ✔ Zug, Switzerland (Serverbase Gmbh) — D4B1Gch4l13nG3f0Rl3753ncRyP7f0Rmy0wN41c434r ✔ Melbourne, Australia — D4B1Gch4l13nG3f0Rl3753ncRyP7f0Rmy0wN41c434r	Once your new record propagated*, you can ask "Let's Encrypt" to verify it. *Note : you can verify the propagation process with the following Web sites : dnschecker.org or whatsmydns.net. You can also run the following command : - nslookup -type=TXT acme-challenge.alcasar.mondomain - dig +short -t TXT acme-challenge.alcasar.mondomain
Intégration Let's Encrypt Status : Actif Nom de domaine : alcasar.mydomain.net API : dns Prochain renouvellement : 22-08-2017 17:19:49 [Renouveller (forcer)]	Your ALCASAR uses now your new certificate « Let's Encrypt » for its ciphered flows. You will have to renew that at the expiration date of the certificate.

Via the command line

Creation

1) Ask a certificate for « alcasar.mydomain.net » :

   « `alcasar-letsencrypt.sh --issue -d alcasar.mydomain.net --email my@domain.tld` »
   The challenge is saved in the file "/usr/local/etc/alcasar-letsencrypt"
2) On the Web site of your registrar, modify your DNS zone, adding a new TXT record named "_acme-challenge..." which the value is the challenge (see previous step). Note : you must wait for the propagation process.
3) Ask for the validation :
   « `alcasar-letsencrypt.sh --renew` »

If the validation process succeeds, you receive your certificate file. The script writes it directly in the right directory of ALCASAR (note : All devices connected on the consultation network should be rebooted).

Automatic renew

The script can create and remove the DNS records automatically via your registrar API (when he has one). You can verify that the script knows your registrar API in the folder "dns_myapi" with the following command :
« `API_Key="XXXXX" alcasar-letsencrypt.sh --issue --dns-api dns_myapi -d alcasar.mydomain.net --dnssleep 10` »

Note : the "`--dnssleep [second]`" parameter is used to set the time between the record creation and the validation (propagation time).

7.5. <u>Use of an external directory server (LDAP or AD)</u>

ALCASAR embed a module for 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 requested.

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

Remark :
- attributes of users stored in the external directory (like the passwords) 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 for the login name unlike the local database of ALCASAR.

<u>Examples of an A.D.:</u> This screenshot shows how the directory is organized. The place where standard users are saved has the following Distinguish Name (DN) : 'dc=Users;dc=serverad;dc=com'. The account name used by ALCASAR to request the directory is "alcasar". This standard account just need to read the directory remotely (add the delegate control "Read All properties" to this user). Beware that this account must not change its password at the first login.

- <u>DN of the base</u> : 'dc=Users;dc=serverad;dc=com'. This DN set the position where searching the users.
- <u>UID</u> : 'sAMAccountName' for an A.D.; 'uid' in general for other LDAP servers.
- <u>User search filter</u> : leave this field empty unless you want to select only specific users.
- <u>User operated by ALCASAR</u> : it's the 'DN' of the account used by ALCASAR to read the directory remotely: 'dc=alcasar;dc=serverad;dc=com'
  Please note that this field and the field "Password" can be left blank if the directory server accepts requests in anonymous mode.
- <u>Password</u> : password affected to the user operated by ALCASAR.

It is possible to provide some specific ALCASAR attributes (bandwidth, concurrent session, etc.) to all the users of an external directory. To do that, create an ALCASAR group named "**ldap**" (in lower case) for which you set the desired attributes.

It is also possible to assign attributes to a particular account authenticated with an external directory. To do this, create an ALCASAR user <u>with the same login name</u> as in the remote directory for which you set the desired attributes.

If you search for more information about how integrate ALCASAR in a complex A.D. architecture, read the additional papers on our Web Site.
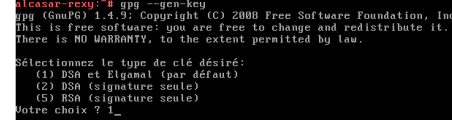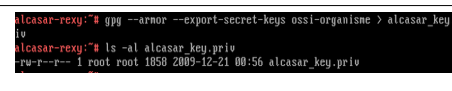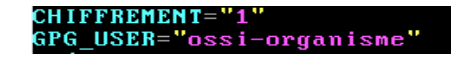
7.6. <u>Encryption of log files</u>

ALCASAR can automatically encrypt weekly log files (cd. §7.1). For this, it uses the GPG asymmetric algorithm (public key + private key).
By providing the private key to an official of your company, you prevent administrators from being accused of log files modification.
In case of inquiry, simply provide log files and the private key for decryption.
The procedure for activating the encryption is as follows:

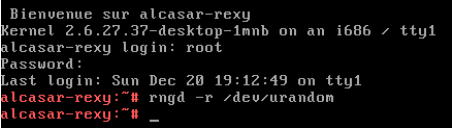| Print screen	Comments	To do
Bienvenue sur alcasar-rexy Kernel 2.6.27.37-desktop-1mnb on an i686 / tty1 alcasar-rexy login: root Password: Last login: Sun Dec 20 19:12:49 on tty1 alcasar-rexy:~# rngd -r /dev/urandom alcasar-rexy:~# _	- Log on as « root ». - Start the entropy generator (random values).	*rngd -r /dev/urandom*

alcasar-rexy: # gpg --gen-key
gpg (GnuPG) 1.4.9: Copyright (C) 2008 Free Software Foundation, Inc.
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.
 	
Sélectionnez le type de clé désiré:
   (1) DSA et Elgamal (par défaut)
   (2) DSA (signature seule)
   (5) RSA (signature seule)
Votre choix ? 1_
	- Generate the key pair (public key + private key).
	- Choose the algorithm, the size and the lifetime of the keys (no expiration).
	- Choose a user name and passphrase.
		gpg --gen-key
		
		info: The user name must not contain spaces. This name is summarized in the term <username> later in this procedure.

alcasar-rexy:~# killall rngd	- Stop the entropy generator.	*killall rngd*
alcasar-rexy:~# gpg --armor --export-secret-keys ossi-organisme > alcasar_key.priv alcasar-rexy:~# ls -al alcasar_key.priv -rw-r--r-- 1 root root 1858 2009-12-21 00:56 alcasar_key.priv	- Export the private key. Copy this to an external media. - Provide it (with passphrase and username) to an official of your organization (Private key escrow).	*gpg --armor –export-secret-key \ <username> > alcasar_key.priv* info : cf. installation doc for the USB management.
alcasar-rexy:~# rm -f alcasar_key.priv alcasar-rexy:~# gpg --delete-secret-key ossi-organisme gpg (GnuPG) 1.4.9: Copyright (C) 2008 Free Software Foundation, Inc. This is free software: you are free to change and redistribute it. There is NO WARRANTY, to the extent permitted by law. sec 1024D/C0D8D6EB 2009-12-20 ossi-organisme Enlever cette clé du porte-clés ? (o/N) o C'est une clé secrète ! - faut-il vraiment l'effacer ? (o/N) o	- Delete the previously generated keys - Delete the private key from the GPG keyring	*rm -f alcasar_key.priv* *gpg --delete-secret-key <nom_utilisateur>*
CHIFFREMENT="1" GPG_USER="ossi-organisme"	- Enable encryption by changing the variables "CRYPT" and "gpg_user" in the file « */usr/local/bin/alcasar-archive.sh* ».	*vi /usr/local/bin/alcasar-log-export.sh* 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 -files <filename_crypt_archive>*'.

7.7. Managing multiple Internet connections (load balancing)

ALCASAR has a script to distribute requests over a number of gateways to the Internet *"alcasar-load_balancing.sh start | stop | status"*.
The parameters are not included in the ACC, it is necessary to modify the global configuration file *"alcasar.conf"* located under *"/ usr / local / etc"*.
Associated parameters (virtual network cards, weights, gateway ip address, etc.) must be defined in the following format: WANx = "active [1 | 0], @ IPx / mask, GWx, Weight, MTUX".
The script creates the interfaces on the fly.
To make it active, the parameter "MULTIWAN" must include the "on" or "On" value; otherwise insert the "Off" value to enable the "single gateway" mode.
The connection test frequency is set by default to 30 sec.
Please note:
The parameter "FAILOVER=0" enables the MULTIWAN mode with no connection test to the gateways (no gateway failure detection).

7.8. Creating an ALCASAR dedicated PC

This chapter presents an example of a dedicated PC ALCASAR (appliance) whose constraints are : miniature (mini-itx), low noise, low cost and low energy consumption.

The configuration is the following :
- Case mini ITX (12V powerline);
- motherboard with dual Ethernet card and an onboard Intel-Celeron processor
    ◦ Gigabyte N3150N-D3V or C1037UN
- 4GB or 8GB of DDR3 SODIMM memory;
- HDD 2.5' 200GB SATA.

SSD

Memory : 4GB of DDR3

The cost of this configuration is around 250 € (shipping included).
The 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 deployed, the unit requires no keyboard, no mouse and no screen.
See also : Qotom boxes.

7.9. Bypassing the portal

For reasons of maintenance or emergency, a portal bypass procedure was created.
It disables user authentication and filtering.
Logging network activity remains active.
Network event logging remains active, but ALCASAR does not trace internet connections anymore.
- Bypass the portal by running the script « *alcasar-bypass.sh --on* ».
- To stop it, run the script « *alcasar-bypass.sh --off* ».

Please note:
Bypass mode is no longer active after restarting the server.

8. Shutdown, restart, update and reinstallation

8.1. Shutdown and restart

There are three possibilities to stop or restart properly the system:
- Via ACC
- by briefly pressing the power button of the PC;
- by connecting to the console as root and running the command "init 0";

When restarting the portal ALCASAR a procedure deletes all connections that have not been closed due to an unplanned shutdown (failure, power failure, etc.).

8.2. Operating system update

Mageia-Linux provides an excellent mechanism to apply security patches on the system and its components. ALCASAR has been developed to be fully compatible with this mechanism. So, every night at 3:30, the security updates are downloaded, checked and applied. As root, you can manually update the system with the command « *urpmi –auto --auto-update* ».

Once the update is complete, a message may warn you that a system reboot is required. This message appears only if a new kernel or a major library were updated.

8.3. ALCASAR minor updates

You can see if an update is available on ALCASAR web page, or on the cover page of the ACC, or by executing the following command « *alcasar-version.sh* ». Download and extract the archive of the latest version like a normal installation.

When starting the installation script (« *sh alcasar.sh --install* »), it detects your current version and offers you the possibility to update automatically ALCASAR to the latest version available.

Only minor updates can be done by that way. If it's impossible, the script ask you to perform a reinstallation. During a minor update, the following settings will still remain:
- network configuration;
- the name and logo of the organization;
- logins and passwords for administrative accounts of the portal;
- users and groups database;
- main and secondary blacklists;
- trusted sites and MAC addresses list;
- network filtering configuration;
- the certificates of the Certification Authority (C.A.) and the server certificate.

8.4. ALCASAR major update or reinstallation

Via ACC, create a backup of the current users database (see §6.2). Save this backup file on another system.
Install the new operating system and the new version of ALCASAR (see installation documentation).
Via ACC, import the user database (see §3.6.a).

9. <u>Troubleshooting</u>

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

9.1. <u>Network connectivity</u>

Retrieve the network information in the file "*/usr/local//etc/alcasar.conf*"
- <u>Check the network card status:</u> run the command "*ip link*" to know the name of your two network cards. In the following of this document, we use "INTIF" for naming the internal network card (connected to the consultation network). "EXTIF" is the name of the external network card (connected to the broadband router). Run "*ethtool INTIF*" and "*ethtool EXTIF*" in order to check the status of both network cards ("*Link detected*" and "*Speed*" fields for example) ;
- <u>gateway/router connection test:</u> Run the command "*route -n*" to display the IP address of the broadband modem/router. Ping the broadband modem/router (Internet router). If an error occurs, check the cable connections and the status of the gateway/router;
- <u>External DNS servers connection test:</u> Ping the DNS servers. If an error occurs, try with another server;
- <u>Internal DNS server connection test (dnsmasq)</u> : Send a name resolution request (ex. : *nslookup www.google.fr*). If an error occurs, check state of the service "dnsmasq". You can restart the dnsmasq service with the command : « *systemctl restart dnsmasq* » ;
- <u>Connection test to the Internet:</u> run the command « *wget www.google.fr* ». In case of success the Google page is downloaded and saved locally (index.html). The result of this test is displayed in the menu "system / service" of the ACC;
- <u>Device connection test</u> : Run the command « *arping -I INTIF @ip_equipment* » to know if a device is connected to the ALCASAR network.
- To discover all the device, install the "arp-scan" package ("*urpmi arp-scan*") and run the command « arpscan -I INTIF --localnet » ;
  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

9.2. <u>Available disk space</u>

If the available disk space is not enough, some modules may not run properly anymore. You can check the available disk space (especially the */var* partition) :
- in GUI-mode via the homepage of the ACC;
- in text mode, using the command « *df* »

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

9.3. <u>ALCASAR server services</u>

In order to complete these tasks, ALCASAR uses several server services. The status of these services is displayed in the ACC (menu « system/services »). You can stop or restart them.

If one of these services can't be restarted, you can diagnose the mistake. Connect to the console of ALCASAR (directly or with SSH). You can control the services with the command « *systemctl start/stop/restart service_name* ». At the same time, display the log file with the command « *journalctl -f* ».

9.4.   <u>Problems experienced</u>

This chapter presents feedback of organizations who have faced problems and have solved them.

a)   **Navigation impossible with some antivirus**

Disable the « proxy-web » function integrated in some antivirus. In Trend-Micro antivirus, for example, this function relies on a whitelist/blacklist downloaded from the servers of Trend Micro (backup30.trendmicro.com, etc.) that analyses/validates each request of a website... A limited rights users can enable it.
To avoid all inconvenience of this function incompatible with ALCASAR, it is better to stop the service « Proxy Trend service » and to restart the computer.

### b)   **Windows clients with static addressing**

It is <u>necessary</u> to add the DNS suffix « localdomain » (Network configuration / Advanced / DNS).

c)   **No Internet browsing but the browser accesses the homepage of ALCASAR (http://alcasar)**
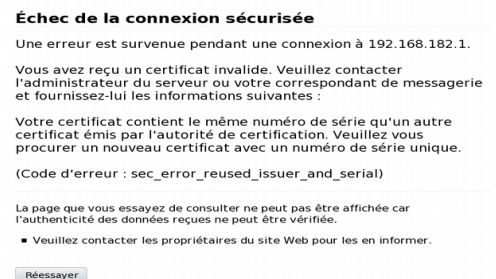
This can occur after a complete reinstallation of the portal or after an update with a change of the server certificate. Browsers display the following pages when they attempt to access a website:
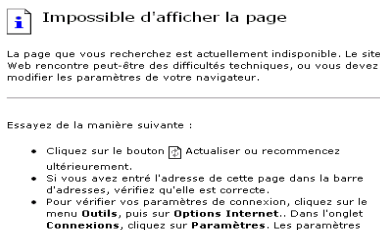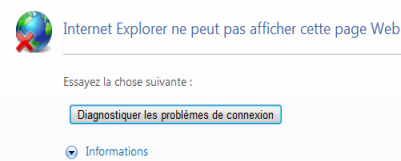
| With IE6 | With IE 7 - 8 and 9 | With Mozilla |

This is because browsers try to authenticate the ALCASAR portal using an old certificate. The old certificate must be deleted on the browsers (« Tools » / « Internet options » / tab « content » / button « Certificates » / tab « Root certification Authority »).

d)   **No Internet browsing but the « Trusted sites » section is filled in**

ALCASAR verifies the validity of domain names entered in this section (cf. § 4.7.a). If a domain name is not valid, the 'chilli' service can no longer start. Then, change the invalid domain name and restart the 'chilli' service with the command « service chilli restart ».

e)   **Operating System and Memory Overload**

The Linux system always attempts to use the maximum amount of memory (RAM) available. On the homepage of the ACC, the bar graph indicating the use of the memory can regularly be beyond 80 percent and can turn red. This is normal. If the system needs more memory, it will use the swap. This swap is an area of the hard disk used when your computer runs out of RAM but this "memory" is approximately 1000 times slower. If you notice that the system uses swap space (> 1%), you can consider increasing the RAM to significantly improve system responsiveness especially when the domain names and URLs filtering is enabled. You can display the system load on the home page of the ACC in 'System /Load system', or in a console with the commands « top » or « uptime » :
  · 3 values shown represent the average system load average for the last hour, the last five hours and the last 15 minutes. The average load is the number of processes waiting for CPU usage. These values are normally less than 1.
  · A value greater than '1 .00' results from an undersized server (especially if it affects the three values (long-term overload).
  · Search the process which represents a high proportion of the load (command « top »).

9.5. Server optimization

In the case of large networks, Internet delays can be detected while the system does not seem to be overloaded (see main page of the ACC: load average <1, no or little use of the area swap processor operated 'normally', etc.).
Check your bandwidth while Internet access is compatible with the number of users simultaneously connected (throughput per user = overall throughput / number of connected users).
These delays can occur especially when the filter attributes are enabled (blacklist / whitelist).
Depending on the physical capabilities of the server, it is possible to attempt to optimize certain parameters.
Several of them have already been integrated in the 2.9.2 version of ALCASAR, but they can be adjusted to better stick to your architecture. It will be good to test over a short period before validating the parameters.
The services on which it is possible to act are:
- The instance of "dnsmasq-blacklist" by increasing the buffer size (256MB by default). To increase it to 2048MB add value *cachesize 2048* in */etc/dnsmasq-blacklist.conf* .
- The "dansguardian" service the number limit "son process" can be reached quickly. In */etc/dansguardian/dansguardian.conf* file, you can assign the following values:
  - *Maxchildren = 500*
  - *Minchildren = 30*
  - *Minsparechildren = 24*
  - *Preforkchildren = 10*
  - *Maxsparechildren = 256*
  - *maxagechildren = 10000*
- The antivirus service "havp" which is directly related to the Dansguardian service. In */etc/havp/havp.config*, you can assign the following value: *SERVERNUMBER 30*

To take into the changes, restart the services:
- *systemctl restart dnsmasq-blacklist*
- *systemctl restart dansguardian*
- *systemctl restart havp*

On the main page of the ACC, check that the "Load Average" setting does not increase beyond measure; otherwise decrease parameters at once.

10. Security hardening guide

On the consultation network, ALCASAR is the Internet Access Controller. It also helps to protect the network from external threats or from internal usurpation. To this end, it includes :
- protection credentials theft. The authentication flow between devices and ALCASAR users are encrypted. Passwords are stored encrypted in the database of users;
- protection against forgetting to log out. The users whose the equipment don't answer for 6 minutes are automatically disconnected; moreover, the attribute "time limit of one session" (cf. § 4.1) allows to automatically disconnect a user after a pre-set time;
- protection against session hijacking by spoofing network settings. This spoofing technique exploits the weaknesses of "Ethernet" and WIFI protocols. To reduce this risk, ALCASAR incorporates an auto-protection process which is running every 3 minutes (*alcasar-watchdog.sh*);
- antiviral protection using an antimalware running on the WEB flows (HTTP) of the users who are the attribute is set;
- several filtering systems and anti-bypass systems (DNS proxy, dynamic firewall, evolutive blacklists (IP addresses, domain names and URLs), configurable whitelists.

The mere presence of ALCASAR not guarantee an absolute security against all threats, including internal threat (hacker on the ALCASAR network). In most cases, this threat remains very low. Without being paranoid and if you really need a high security, the following measures can improve the overall security of your system.

10.1. On ALCASAR

- Choose a strong "root" password (you can change it by running the command « *passwd root* ») ;
- Protect your "ALCASAR" server and ISP's equipment to prevent unauthorized access, theft or installation of equipment between the modem and ALCASAR (locked premises, padlocks, etc.);
- Configure the BIOS so that only the internal hard disk drive is bootable;
- Set a password to access the BIOS setup.

10.2. <u>On the network</u>

a) Network type "hotspot"

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 of these computers (like "cybercafe" computers). These products allow the user to be compartmentalised in a sealed environment. At the end of his session, the user environment is totally cleaned.

- On Linux, you can install the product "xguest" (it is provided natively with Mageia, Mandriva, Fedora, RedHat and Centos distributions)
- On Windows, you can chose one of these not free projects : *"Openkiosk", "DeepFreeze", "Smartshield" and " reboot restore RX". They save all the computer and restore it after a reboot.* Microsoft gave the software "Steady state" for XP/Vista. This software is no longer supported.

On WIFI Access Points (AP) :

- Enable the "client isolation" option (also called wireless isolation). It prevents a user connected to an access point to communicate with another one connected to the same access point. They can only connect to Internet via ALCASAR.
- Enable WPA2-Personal encryption (also known as WPA2-PSK). It avoids users 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.

On switches of wired Ethernet networks :

- 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 strong key;
- on Ethernet switches:
  ○ Enable the "lock port" ("Port Security" function) to associate the MAC addresses of devices to the physical ports of switches;
  ○ select the "DHCP snooping" function on the port used by ALCASAR and on the interswitch ports. This will prevent false DHCP servers (Fake DHCP servers).

Devices can (should) incorporate several security features such as locking the BIOS setup, locking the desktop configuration, antivirus, automatic update security patches (patch), etc. To facilitate downloading of security patches or antivirus updates (cf. § 4.7), ALCASAR can authorize devices to automatically connect without authentication on sites specifically identified.

Make your users aware of these two security features:

- **Password must be changed**
- **Credentials must remain confidential (Each user is responsible of "friend's session" using his credentials).**

11. __Annexes__

11.1. __Useful commands and files__

The administration of ALCASAR can be done from a command line interface (as 'root'). All these commands (shell scripts) begin with "alcasar-... " are located in the directories « */usr/local/bin/* » and « */usr/local/sbin/* ». Some of them rely on the central configuration file of ALCASAR (« */usr/local/etc/alcasar.conf* »). The "-h" argument lists available command line arguments.

- **alcasar-activity-report.sh**
  - create the weekly graphical activity report. This script is send by crontab every sunday at 5.35pm.
- **Alcasar-archive.sh**
  - [-l|--live]: create the archive file (named 'traceability') of the users log files and the users database for the last day;
  - [-n|--now]: create the archive file (named 'traceability') of the users log files and the users database for the last week (launch by cron every monday at 5:35 pm);
  - [-c|--clean] : remove archive files older than one year.
- **alcasar-bl.sh**
  - [-download|--download] : download the latest version of the BlackList (BL);
  - [-adapt|--adapt] : adapt the freshly downloaded BL to the ALCASAR architecture ;
  - [-reload|--reload] : activate the freshly downloaded BL;
  - [-cat_choice|--cat_choice]: apply changes done via ACC (modifying categories, adding/removing domain names, etc.).
- **alcasar-bypass.sh** [-on/-off] : enables/disables the « BYPASS » mode.
- **alcasar-CA.sh** : creates a local CA certificate and a server certificate for the host "alcasar.localdomain". The Web server need to be restarted (*systemctl restart httpd*).
- **alcasar-certificates.sh**: import & export certificates.
- **alcasar-conf.sh**
  - [-create|--create]: creation of an archive file of ALCASAR (/tmp/alcasar-conf.tgz) use when the system is updated;
  - [-load|--load]: load an archive file (don't apply);
  - [-apply|--apply] : apply the parameters of the configuration file (/usr/local/etc/alcasar.conf).
- **alcasar-daemon.sh** : Check the state of the main ALCASAR services (17 in V 2.9.2). Restart those that seem not running. Launch by cron every 18'.
- **alcasar-dhcp.sh** [-on|--on][-off|--off] : enable/disable DHCP service.
- **alcasar-file-clean.sh** : cleanning of several ALCASAR conf files (sort, remove empty lines, etc.).
- **alcasar-https.sh** [-on|--on][-off|--off] : enables/disables HTTPS to authenticate the users.
- **alcasar-importcert.sh**
  - [-i certificate.crt -k keyfile.key (-c certificate_chain.crt)] : import an official certificate of security;
  - [-d] : go back to the auto-signed certificate.
- **alcasar-certificates.sh** :
  - [-x] : Export of all the certificates of the portal in the form of a timestamped archive ;
  - [-i alcasar-certificate-<date:heure>.tar.gz] : Import the set of certificates from an archive or from a backup ; useful during copy out of another server or migration towards a more recent system.
- **alcasar-iptables.sh** : apply the ALCASAR iptables rules to the firewall.
- **alcasar-load-balancing.sh** : Aggregates several Internet connections. IP addresses, bandwidth and MTU of available modems/routers must be configured in the file */usr/local/etc/alcasar.conf"* to work properly. Remember, the script is automatically launched when the system starts up <u>only</u> if the MULTIWAN parameter is set up in the file *"/usr/local/etc/alcasar.conf".* To ensure the script is running properly, execute the command : *ip route*. ("start", "stop" and "status" are the options available for this command).
- **alcasar-logout.sh**
  - [username] : logout the user <username>;
  - [all] : logout all the logged users.
- **alcasar-mysql.sh**
  - [-i file.sql | --import file.sql] : import a users database (! overwrite the existing one);
  - [-r|--raz] : reset the users database;
  - [-d|--dump] : create an archive file of the current users database in « /var/Save/base » ;
  - [-a|--acct_stop] : stop the open accounting sessions;
  - [-c|--check]: verify the integrity of the users database and try to repair it if needed.
- **alcasar-nf.sh** [-on|--on][-off|--off] : enable/disable the filtering of network protocols;
- **alcasar-profil.sh**
  - [--list
- **alcasar-rpm-download.sh** : downloads and creates an archive file of all the needed RPM to install ALCASAR (/root/rpms-arch.tar.gz). Use this file if you want to install an ALCASAR on a very tiny bandwidth.
- **alcasar-sms.sh** : manage gammu process when a 2G/3G adapter is detected.
- **alcasar-ticket-clean :** remove pdf tickets (vouchers) generated when a user is created (launched by cron every 30').
- **alcasar-uninstall** : remove ALCASAR (used when an update is performed).
- **alcasar-url_filter.sh**
  - [-safesearch_on|-safesearch_off] : enable/disable the safesearch system on search engine (Google, Bing, etc.);
  - [-pureip_on|-pureip_off]: enable/disable the filtering of URLs containing IP addresses (instead of a domain name).
- **alcasar-urpmi.sh** : install and update ALCASAR needed RPMs (used during the installation process).
- **alcasar-version.sh** : display the current version and the last available.
- **alcasar-watchdog** : test the Internet connectivity. Test if an authenticated user isn't usurped (launched by cron every 3').

11.2. <u>Helpful authentication exceptions</u>

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

- The following values allow client devices to access the Internet without authentication in order to connect to the following services:
- perform a test of Internet connection,
- Microsoft system update,
- "TrendMicro", "Kaspersky" and "Clamav" antivirus update,
- check Mozilla version and its modules,
- ...

These exceptions to the authentication process (trusted Web sites) can be set via the ACC (cf. §3.8.a)

- *microsoft.com, msftncsi.com et windowsupdate.com*
- *trendmicro.de et trendmicro.com*
- *update.nai.com, akamaiedge.net et akamaitechnologies.com*
- *clamav.net*

11.3. <u>User sheet</u>

Internet access control

An Internet access control is deployed in order to be complient with the local rules and the law.
This control is performed with ALCASAR (Open source Software) in accordance with privacy principles.

To see the authentication page, connect your Web browser on a **not ciphered** Website (HTTP) like nerverssl.com or euronews.com or on the ALCASAR welcome page (alcasar.localdomain).
Info : Make sure you have disabled the proxies in your Web browser configuration.

The following window will be displayed.

Info: Both fields are case sensitive ("smith" and "Smith" are two different users).
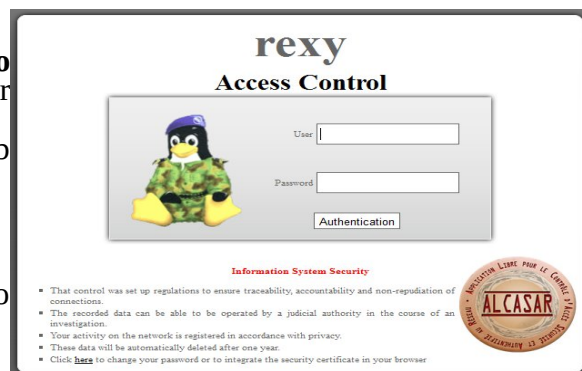
If you want to change your password or install ALCASAR certificate in your Web browser.
You can display this page with the following URL: « alcasar.localdomain ».

When login is successful, this new tab appears. It allows you to logout from ALCASAR (closing connection). This window provides information on your account permissions (lease time, download limits, connections history, etc.).

If you close this tab, you will be automatically disconnected.
You can also log out with the URL "http://logout" in your browser address bar.

The portal embeds a WEB flow antimalware and a website filtering to prevent unauthorized web browsing. It also helps to know if there is a problem with the Internet connection (hardware failure or ISP network failure).
The following Webpages can be displayed: