USER MANUAL

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

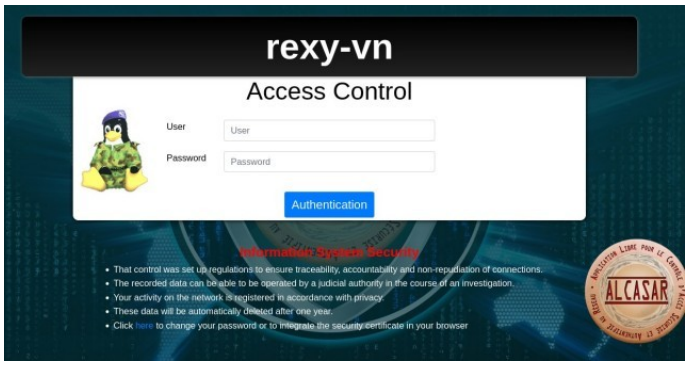
Project : ALCASAR	Author : Rexy and 3abtux with support of « ALCASAR Team ».
Object : User manual	Version : 3.7.1
Keywords : captive portal, access control, accountability, traceability, authentication	Date : 2025 may

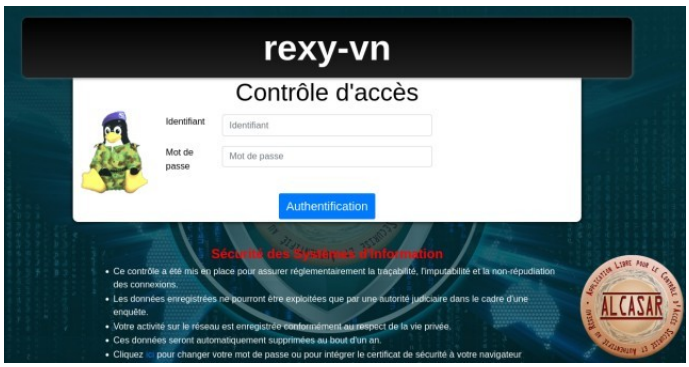
Table of contents

1. Introduction

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

The following screenshot is displayed for users. This page is available in English, Spanish, German, Dutch, French, Portuguese, Arabic and Chinese depending on the browser's settings. As long as the user is not logged in, no traffic will pass through ALCASAR.



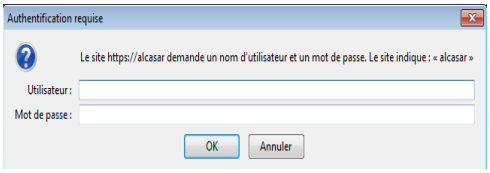


The homepage of the portal is available for any browser connected on the network. By default, the URL is http://alcasar.lan. From there, users can log on, log out, change their password and install the authority security certificate into their web browsers.

Administrators can access the graphical **A**LCASAR **C**ontrol **C**enter (**A.C.C**) by clicking the little notched wheel at the bottom right of the page (or via https://alcasar.lan/acc/). The network flows are ciphered (HTTPS). With Firefox, you can connect accepting a "authentication exception". For other web browsers, see §2.3 to configure them.

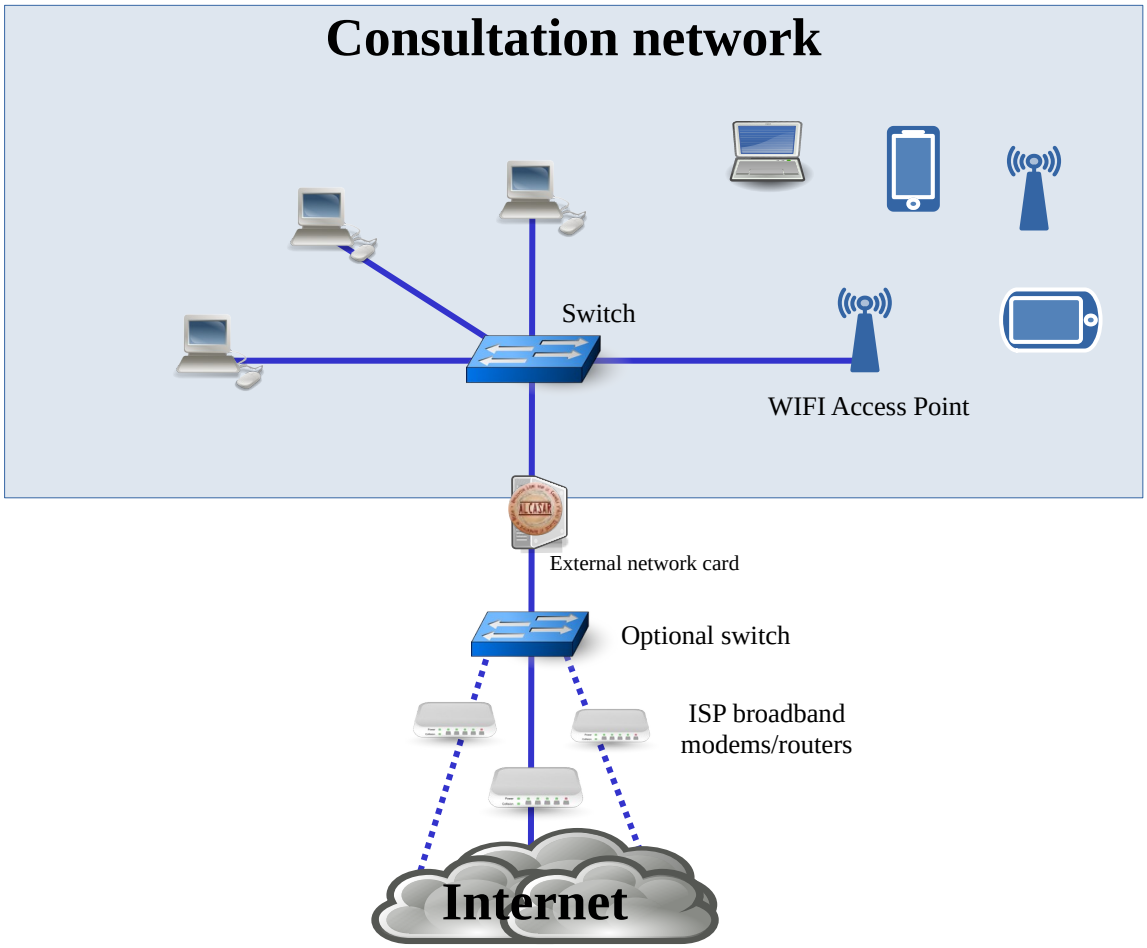
ACC is available in three languages (English, Spanish and French). Authentication is required with a login name in one of the three following profiles (cf. §7.1) :

- 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 architecture



On the ALCASAR network, devices can be connected with multiple technologies (wired Ethernet, Wi-Fi, PLC, etc.). For all these devices, ALCASAR is the Domain Name Server (DNS), the time server (NTP), the network parameters server (DHCP) and the default gateway.

CAUTION : On the consultation network, no other gateway (router) should be present. Verify that your WIFI Access Points are in "bridge" mode.

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

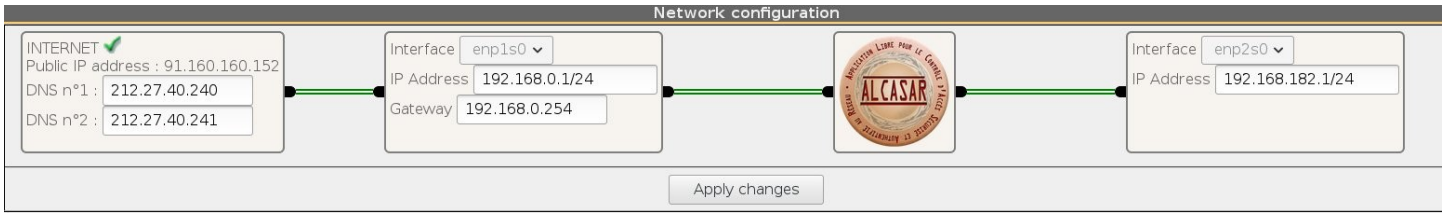
For example, with a class C network (default configuration)

- 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 : "lan" (this DNS suffix must be set in the static address setting of the client device) ;
  - 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 network settings

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

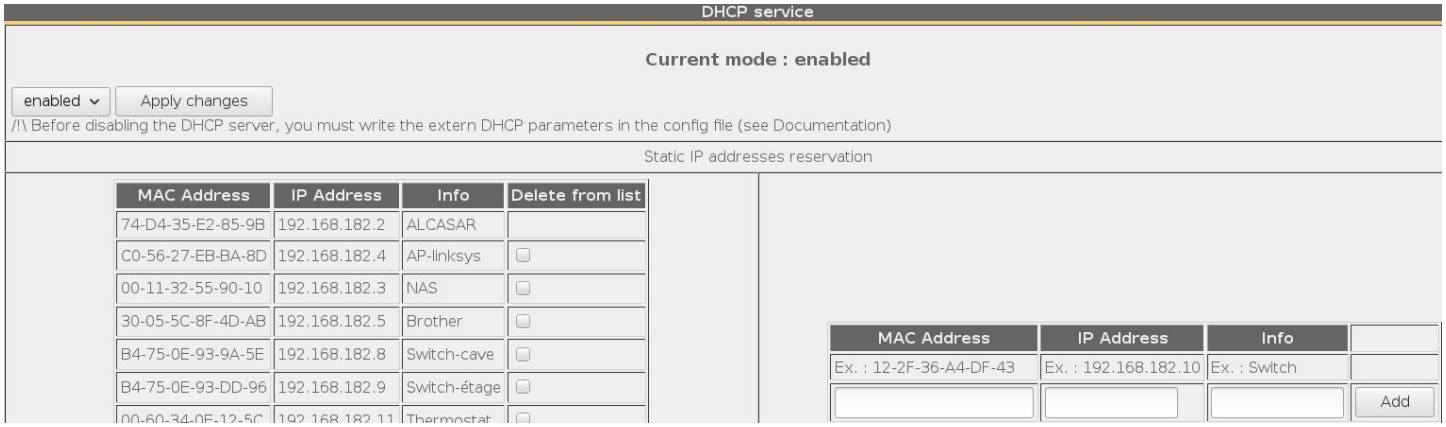
a) IP configuration



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-network.sh --apply* ».

b) DHCP server



The DHCP (Dynamic Host Control Protocol) server embedded in ALCASAR provides dynamically IP settings to client devices connected to the network.
You must warn this DHCP server if you have devices that use static IP addresses (servers, printers, Wi-Fi Access Point, switches, etc.). This avoids IP conflicts.
Be sure that no other router or DHCP server is connected to your network. Or be sure to well knowing how manage multi-DHCP service (cf. §7.5 to manage the cohabitation with a A.D. © server).

c) Local name resolution

As ALCASAR is the name server (DNS) on your LAN, you can ask it to resolve the name of your network equipment in order for 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. Parameters of the consultation network equipment

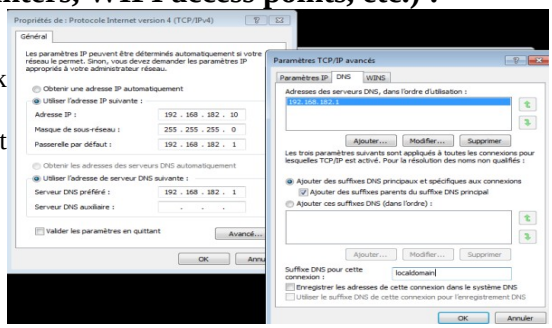
a) User's equipment

A "User sheet" is available at the end of this manual.
Users only need a system in **DHCP mode** and a browser supporting **« JavaScript »**. The **proxy** settings must be **disabled.** To be intercepted by ALCASAR, browsers must try to access an **HTTP** (not HTTPS) website. If they are not automatically intercepted, they can connect to the main portal web page with the following URL: http://alcasar.lan.

b) Adding bookmark

On browsers, it can be useful to add ALCASAR homepage (http://alcasar.lan/) 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 §).

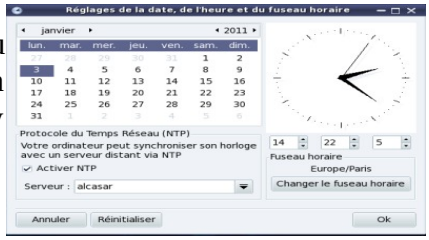
c) Network configuration in static mode (servers, printers, WIFI access points, etc.) :



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 : lan**

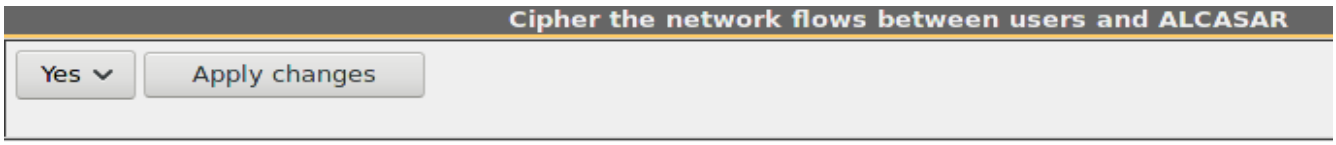
d) Time synchronization



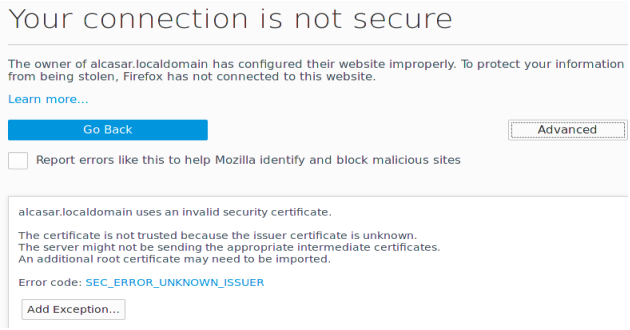
ALCASAR includes a network time-server (« NTP » protocol) allowing you to synchronize devices connected to the ALCASAR network. Thus, on Windows or on Linux, you can define ALCASAR server as the time-server by right-clicking on the clock of the desktop. Enter « alcasar.lan ».

e) Encryption of network flows

Network flows to access the ACC are always encrypted. On the other hand, after its installation, ALCASAR is not configured to encrypt user authentication flows. By leaving this mode, you accept the eavesdropping risk by a malicious user connected to the consultation network. You can enabling or disabling the encryption of the authentication flow via ACC : menu "System" + "Network" of ACC. You can also use the script "alcasar-https.sh {--on|--off}".



This cipher protocol uses TLS (Transport Layer Security) with a security certificate created during the installation of ALCASAR. By default, browsers don't know the authority which has signed the security certificate (we speak about an auto-signed certificate). So, one of the following pages is displayed when they communique with ALCASAR for the first time:

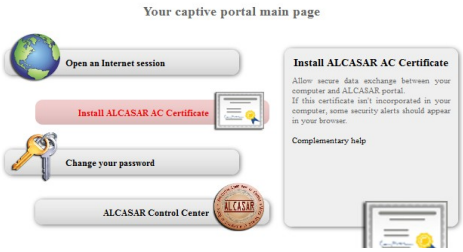


« Mozilla-Firefox »

« Google-chrome »

Three solutions can be used to avoid the warning windows on web browsers :

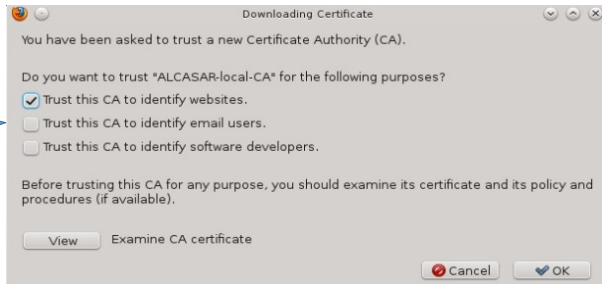
- Leave ALCASAR in its initial configuration. In this case, it is possible to reduce the risk related to flow interception techniques (see §10.2) ;
- Get and install an official certificate (see §7.4) ;
- Keep the original certificate and install in the browsers the certificate of the security authority. To do that, click the zone « Install ALCASAR AC certificate » of the ALCASAR homepage to download this certificate (file: « *certificat_alcasar_ca.crt* »). For each browser, follow the following steps :



« Mozilla-Firefox »

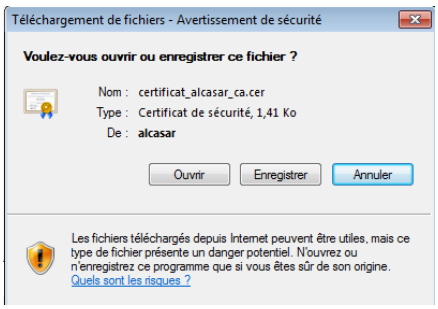
From the Firefox menu, select "options". From the “Privacy and Security” section, select "View Certificates". From the “Authorities” tab, import the downloaded certificate.

Select « Trust this CA to identify websites ».

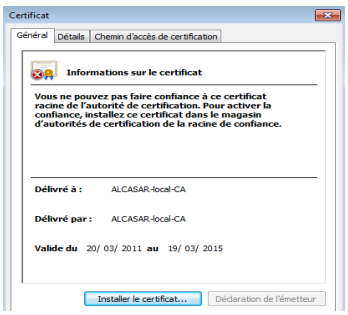


« Edge”, “Chrome » and “Safari”

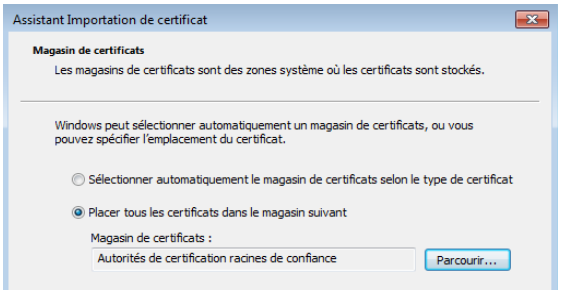
In the browser menu, select « parameters », then “confidentiality”. Click “Manage certificates”. Then « import » in the tab « Authorities ». You can also double-click on the downloaded certificate and follow the next 3 steps :



1 – click « open »



2 – click « install the certificate »



3 – Choose the store « Trusted root certification authorities »

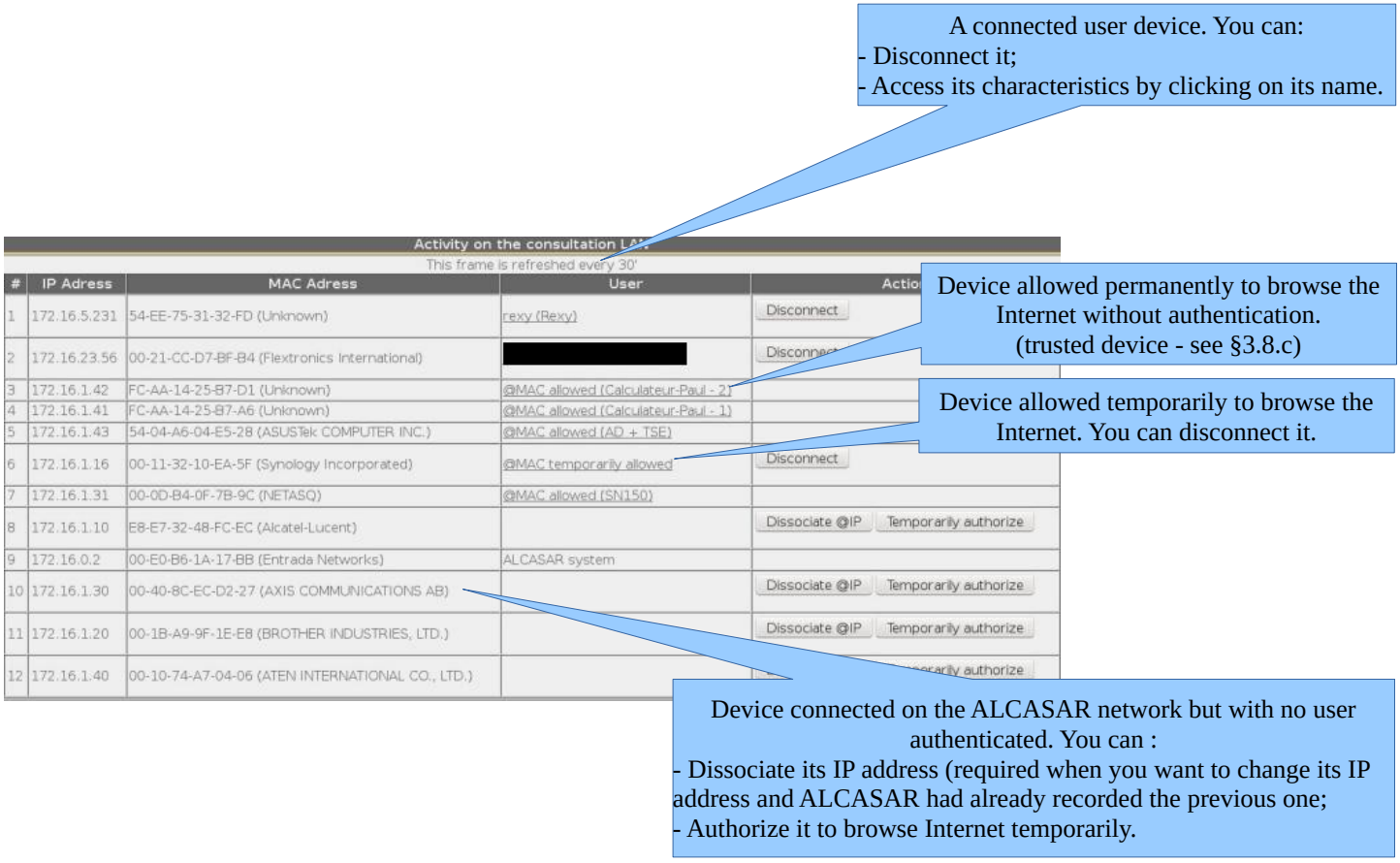
3. Managing users and their devices

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

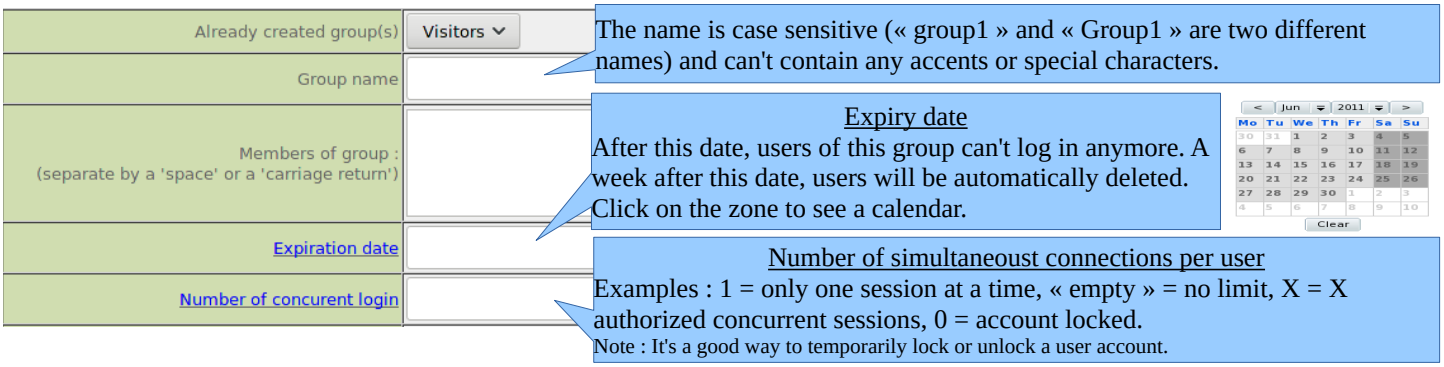
This window displays systems and users on your network.

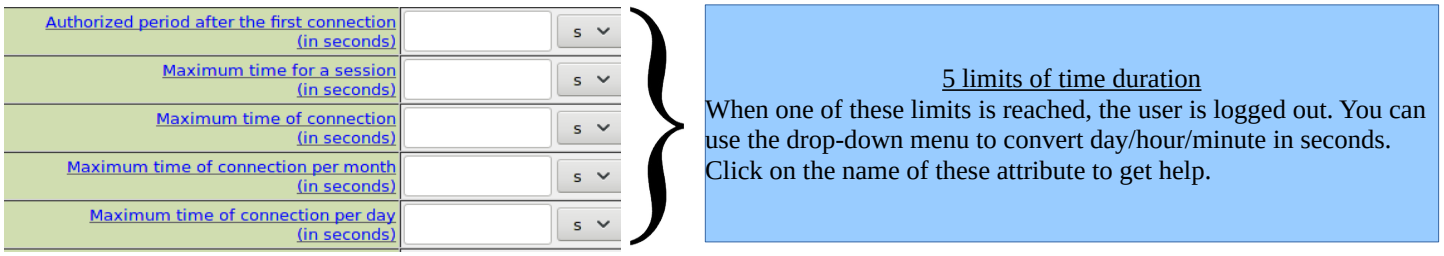


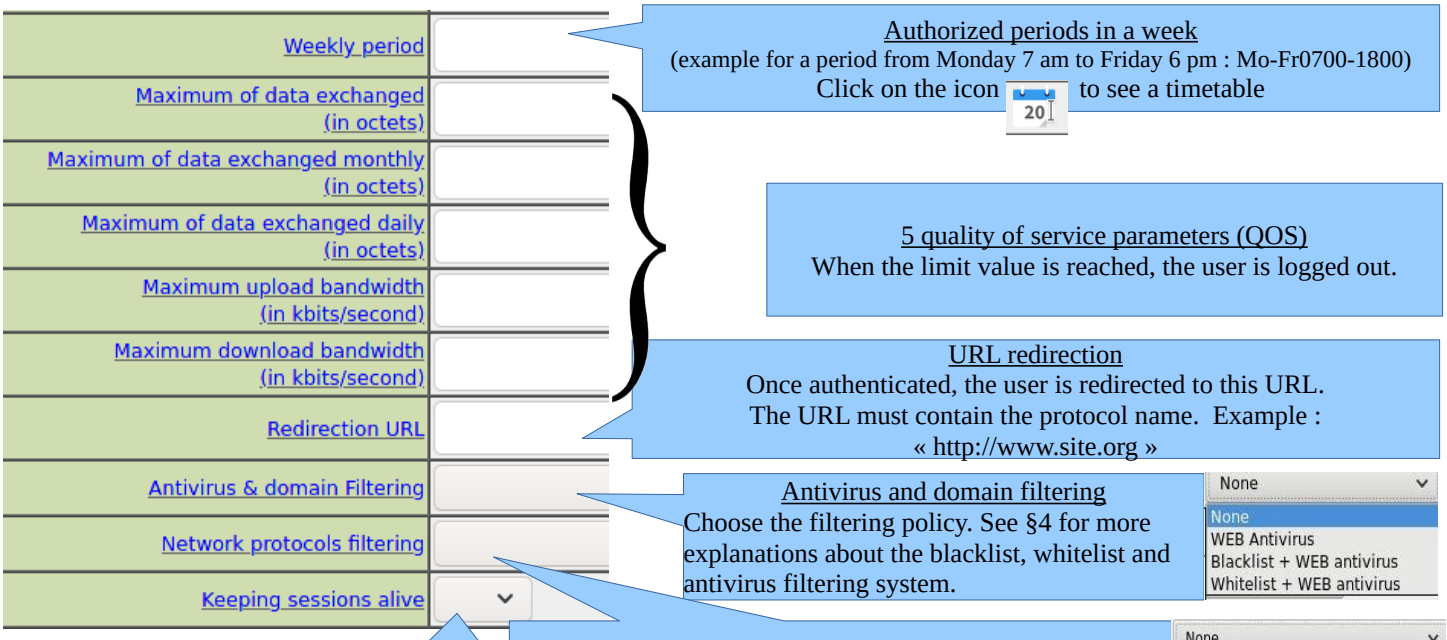
If you see some equipment with IP address “0.0.0.0”, that means that this equipment is configured with a static IP address. You should inform ALCASAR of that situation in adding the IP address of this equipment in the DHCP static table (see §2.1.b).

3.2. Creating groups

Generally, in order to minimize the administration load, it's interesting to manage user groups 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. Let the attribute empty if you don't want to use it. For assistance, click on the attribute name in the left column.
By default all users are in a group named “default”. Create this group name if you want to set some “default” attributes to all your users.

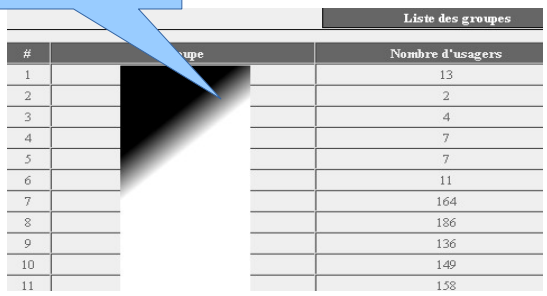


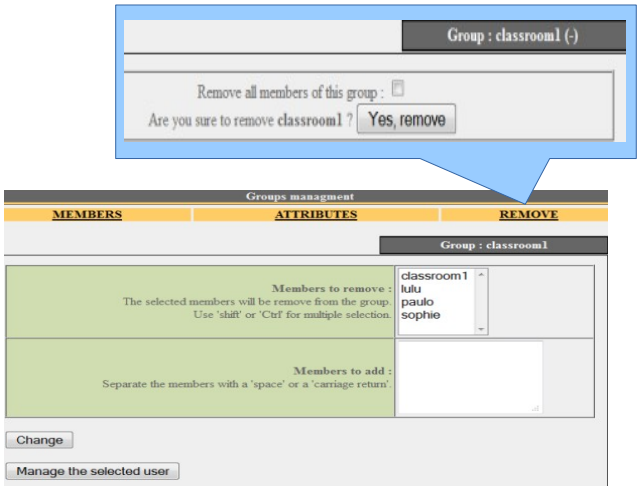




3.3. Editing and removing a group

Click the name of the group to edit it





3.4. Creating users

By default, only most use attributes are displayed. Click on the “Advanced menu” button on the bottom of the page to display all attributes.

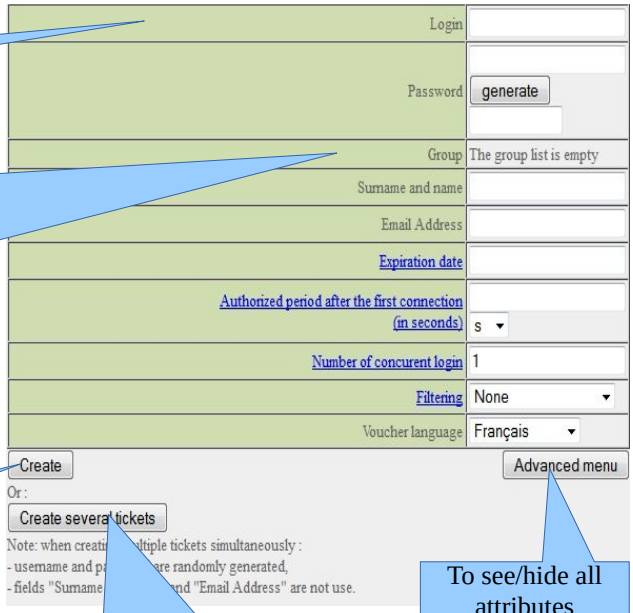
Login and password are case sensitive
(« James » and « james » are two different users)

You can affect a user to a group

- The user inherits of the group attributes.

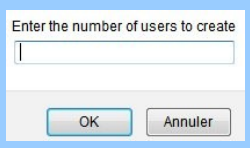
- If an attribute is defined both for a user and for his group, group attributes takes precedence (except for attributes : “concurrent sessions”, “network protocols filtering”, “domain filtering” and “session time”).

- When a user is a member of several groups, you can set his primary group in the user attributes window (see next §).



To see/hide all attributes

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

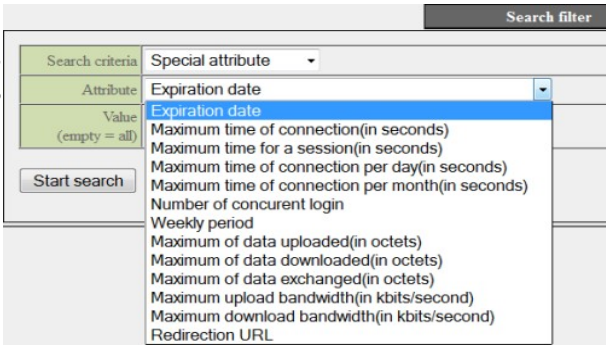


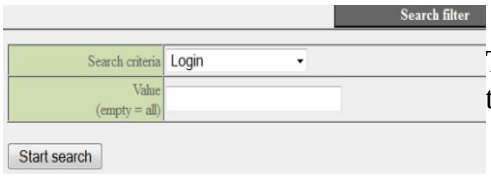
If you create multiple users, it's interesting to fix an expiration date (see the remark below)

Remark : 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. Searching and editing users

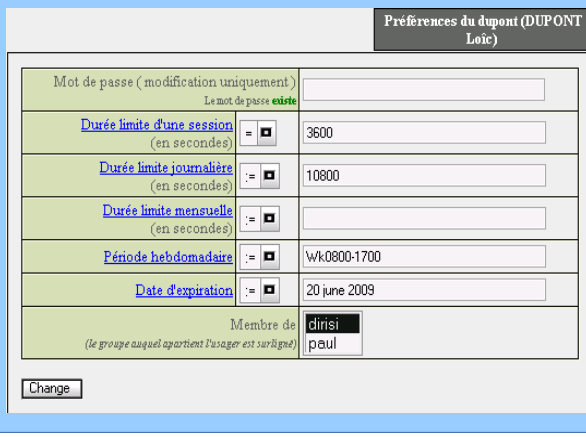
You can search users with several criteria (login name, attributes, etc.). If you leave the criteria field blank, all users will be listed.



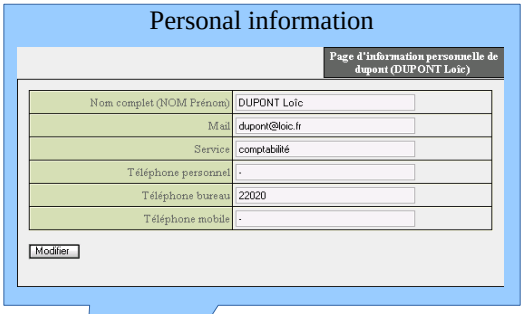


The result is a list of users matching your search criteria. Each user's toolbar includes the following functions :

User attributes

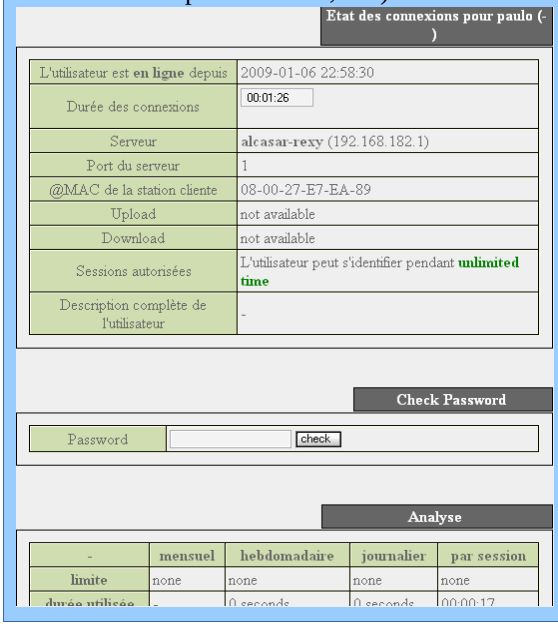


Personal information

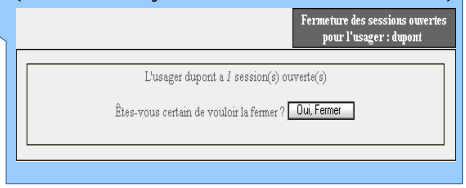


Deleting a user

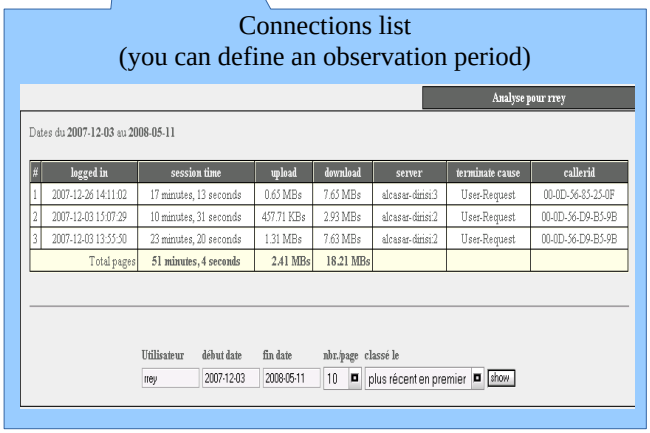
General information (connections list, statistics, password test, etc.)



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

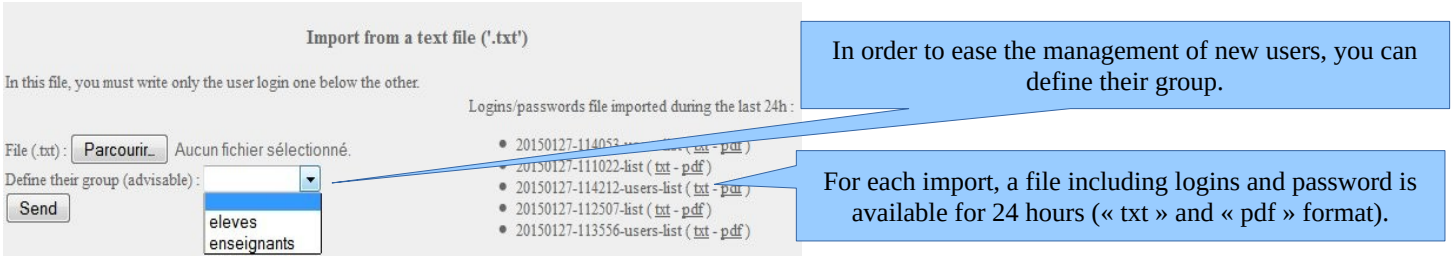
When you import a user database backup, the current database will be emptied. Because this database needs to be provided in case of inquiry, a backup is automatically done (see §7 to retrieve this backup).

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.



3.7. Emptying the user database

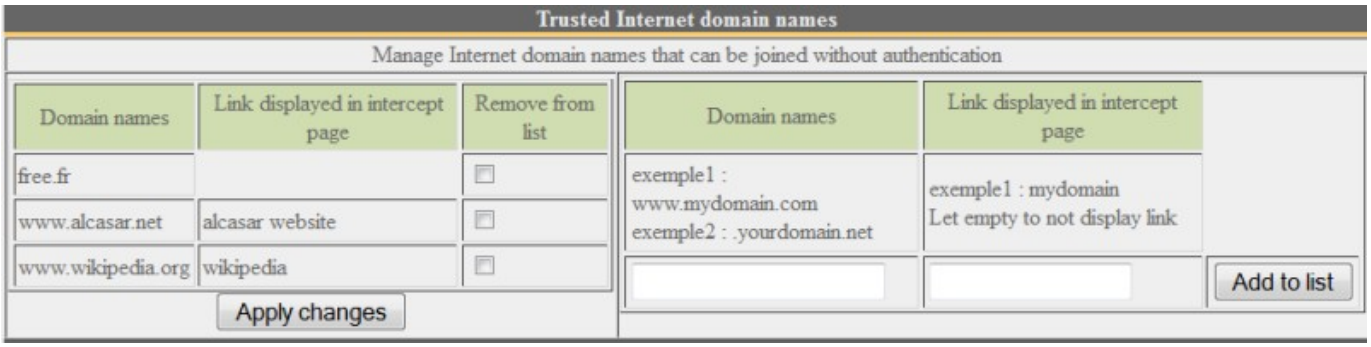
This function allows you to delete all the users in one click. A backup of this database is automatically done. See §6.2 to retrieve the backup. See previous chapter to re-inject it.

3.8. Authentication exceptions

By default, ALCASAR blocks all network flows from viewing equipment without an authenticated user. However, you can define exceptions to this behavior to allow :

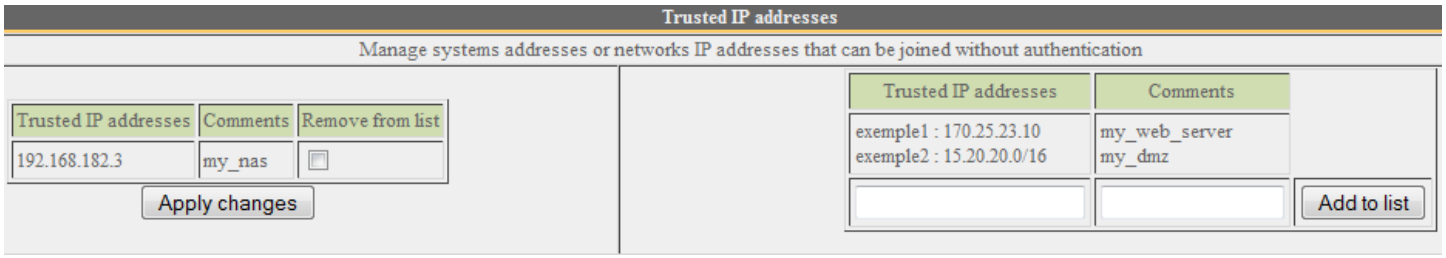
- software and operating systems to update themselves automatically on the editors' websites (cf.§11.2);
- to connect a server or a security zone (DMZ) behind ALCASAR without authentication;
- trusted equipment cannot be intercepted (e.g. PCs/GSMs/tablets assigned to an employee).

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 these 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), has no effect on the addresses mentioned here.

c) Trusted devices

It is possible to authorize some equipment located on the consultation network to pass through ALCASAR without being intercepted. To do this, you need to create a user whose login name is the MAC address of the equipment (written as follows: 08-00-27-F3-DF-68) and whose password is "password".
Connection traces are attributed to the equipment's @MAC.
By entering additional information such as "first and last name" on these accounts, you enrich the MAC address display in the various activity windows (as in the following screenshot: "Headmaster PC", "Vanessa mobile phone", "Pierre tablet", etc.).
This possibility is often named "MAB" (MAC Address Bypass).

3.9. Auto-registration

The objective of these modules is to propose to the users to self-register while assuring the owner of the Internet subscription of the respect of the French legal requirements in terms of imputability (fight against anonymous, non-traceable or ephemeral accounts).

a) By SMS

Purpose, principle and prerequisite

To create this module, we imposed the constraint that ALCASAR should not send any SMS (reception only) so that the operating cost is null and that the licenses of communication operators are respected (standard SIM card).

In order to work, this module required a GSM modem (also called "3G/4G key") with its firmware updated[1], 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.

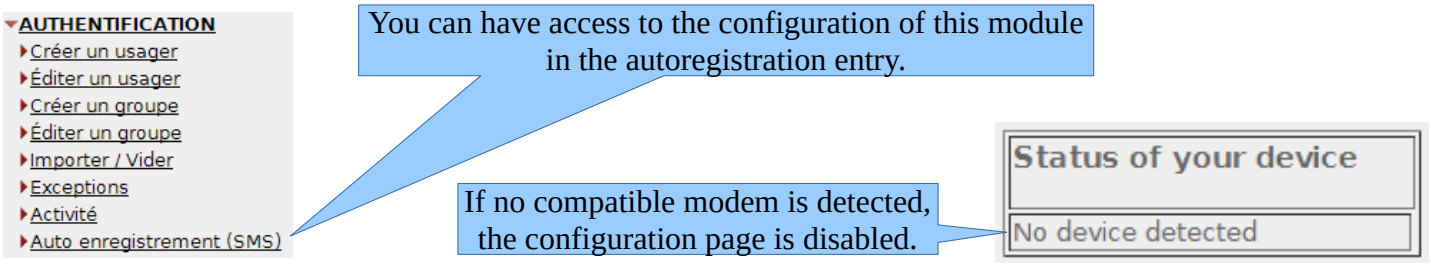
During our tests the following GSM modem was used (average cost: 30€) :

- **« Wavecom fastrack Q2303A » or « OSTENT Wavecom Q2303A »**
  - USB connection port : **ttyUSB0**
  - Connection speed : **9600 bauds**

We detect some issues with Huawei E180, E220 and E372 (communication speed : 115200 bauds). They randomly change their communication ports. Fabien LAFAGE write a post on the following forum : https://adullact.net/forum/message.php?msg_id=487161&group_id=450

Managing the service

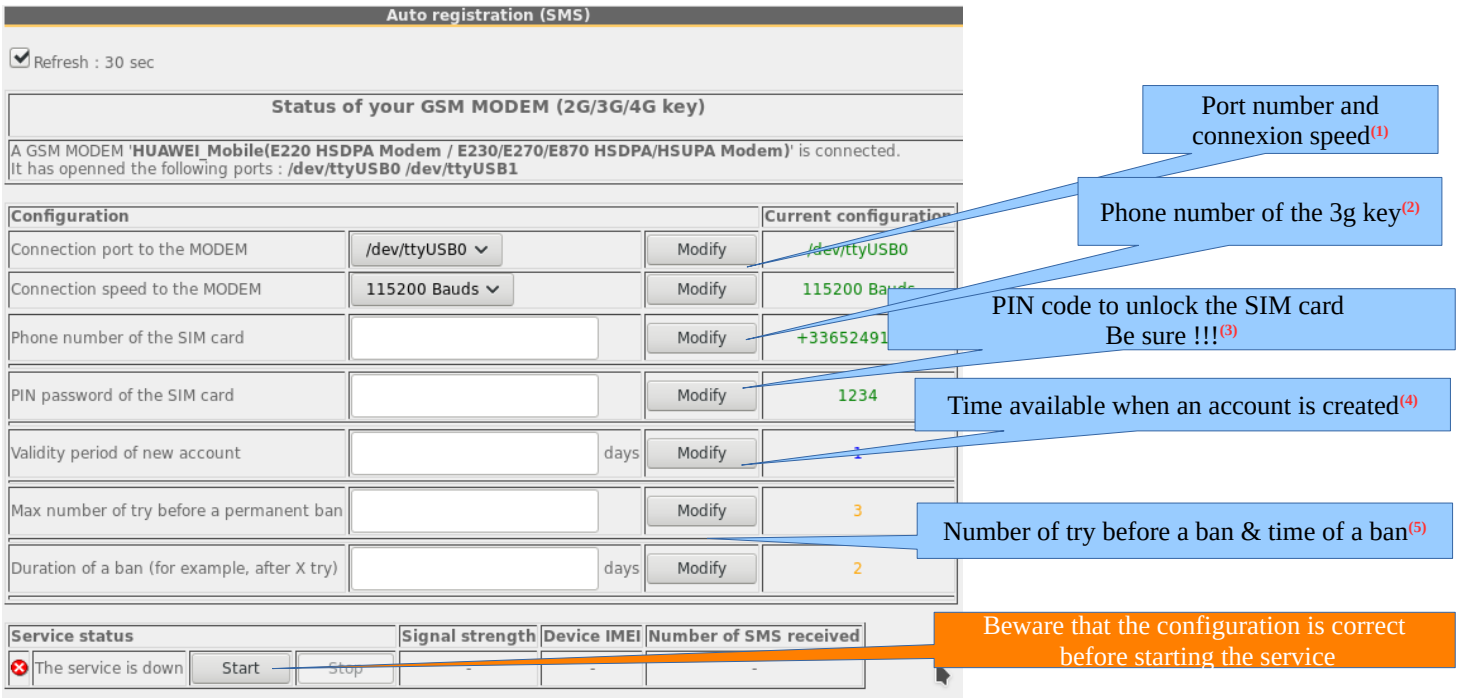
Insert a compatible GSM modem and wait at least 2 minutes for it to finish initialization. Then open the ACC self-registration module.



Before using the GSM modem, test to send and to receive SMS with the SIM card (and PIN password) in a "real" GSM phone.

When a valid GSM modem is connected, **don't start the service before entering the "phone number" and the "PIN password".**

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



(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".

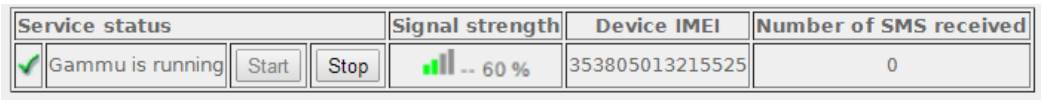
(3) Be careful, if the PIN code is wrong, the SIM card will be locked. In this case, follow the instructions in the technical documentation of ALCASAR (§8.2 Auto-inscription with SMS) to unlock it.

(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.

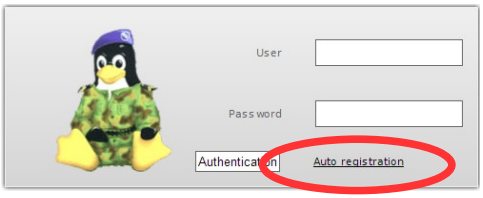
If all is set correctly, you can start the module with the "start" button. Then, wait for about 30'. When the service is started, wait again for the key (recording process on the GSM infrastructure). If all is OK, the service displays the following status:

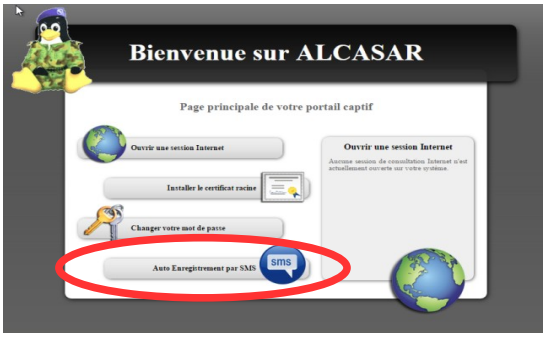


This table shows the status of the service, the signal strength, the IMEI number and the number of SMS received (reset when the service is restarted).

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.



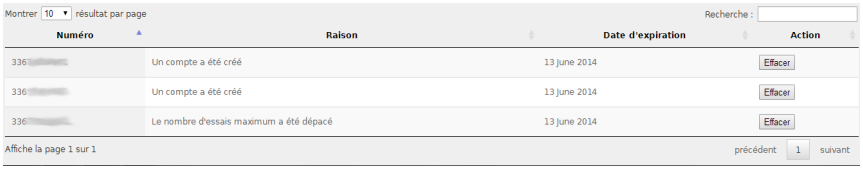


This link gives some information about the SMS account already created. Moreover, each user can have some information on the status of his phone number.

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, but in the following table:

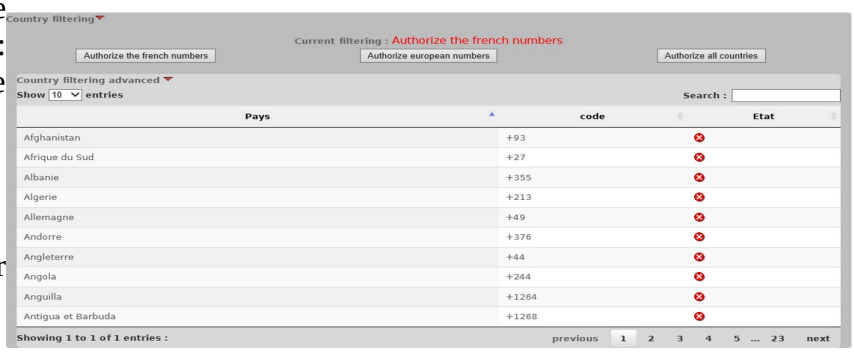
This table gives the state of the phone numbers which have sent one or more SMS. If you click on delete, the account will be deleted and the user can send a new SMS to create an account again.



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.



Error messages [administration]

Cannot listen to 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 ».

b) By E-mail

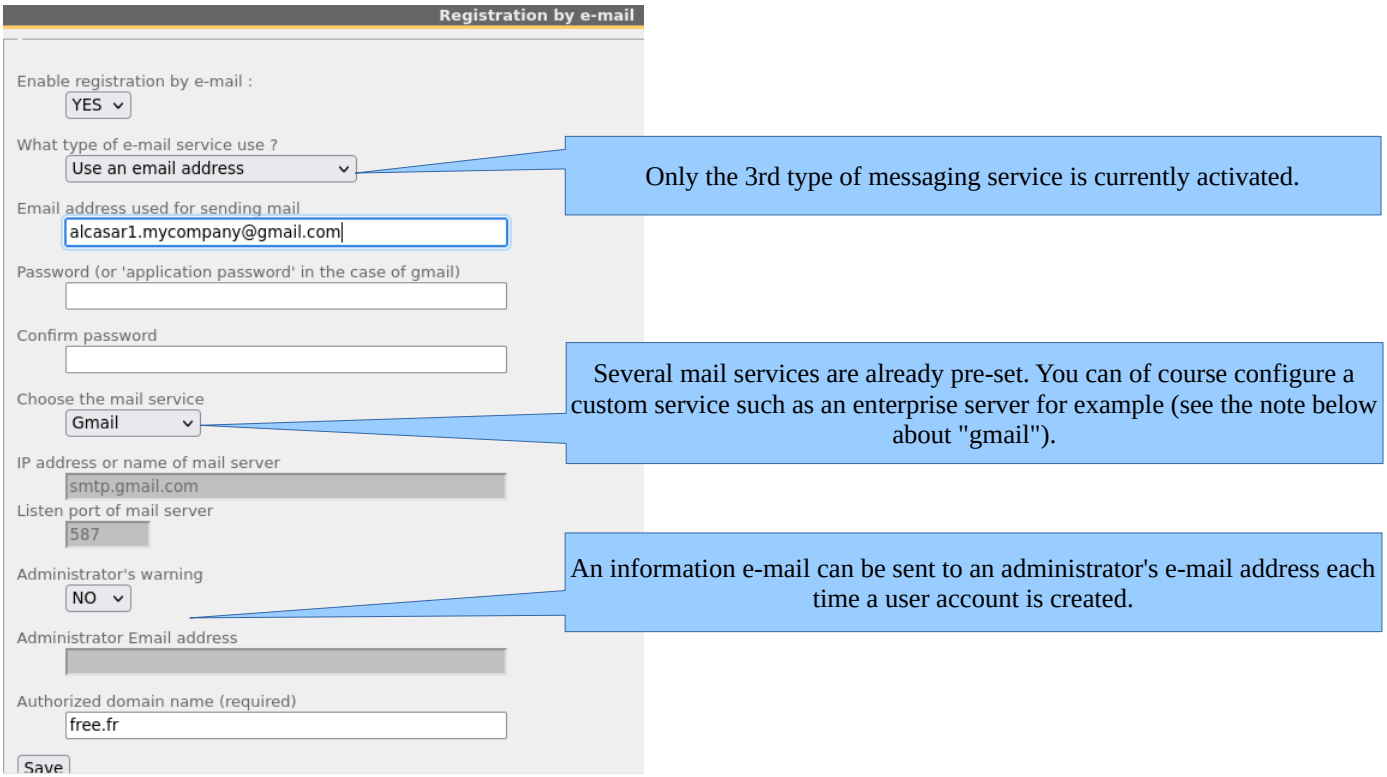
This module allows users to register themselves by entering their e-mail address. They will then receive an email from ALCASAR containing their login details (login=@E-mail and random password). To prevent a user from using an ephemeral or anonymous address, the administrator must configure the e-mail domain name to be the only one authorized (e.g., airbus.com, sncf.fr, etc.).

ALCASAR can send e-mails in 3 different ways (3 types of e-mail service):

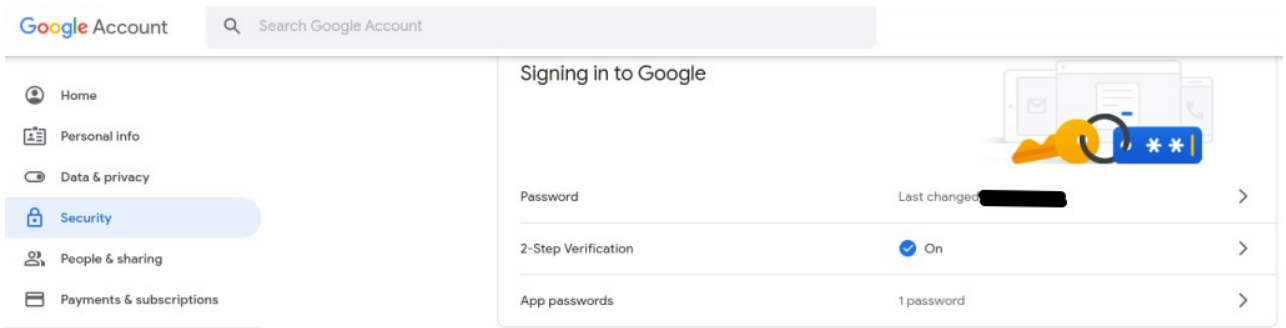
1. it acts as a mail server ;
2. It relays to an external mail server (company server for example);
3. It operates an email account managed by an external server ("free", "sfr", "orange", "Gmail", etc.). In this case, it may be interesting to create a special and representative e-mail account (e.g., alcasar-hotel-esperence@free.fr).

⚠ Since this module is still in experimentation, only the 3e mode is currently enabled.

Managing the service



Note: If you want to use a "Gmail" account, you must substitute the account password with an "application password" that must be created via the administration interface of the Gmail account (myaccount.google.com) menu "security". This "Gmail" account **must first** be configured to use the "two-step verification".



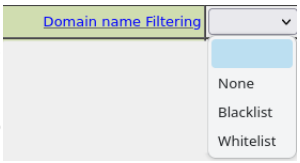
4. Filtering

ALCASAR has several optional filters:

- a blacklist and a whitelist of domain names, URLs and IP addresses;
- a filter for network protocols.

The first filter was developed at the request of organisms likely to welcome young people (schools, secondary schools, recreation centers, parents, etc.). This filter can be compared to the parental control system. You can enable or disable it for each user (or group of users) by modifying users or group attributes (see §3.2 and §3.4). This filter system automatically integrates filtering of search engines (bing, duckduckgo, google, ecosia), YouTube and pixabay.

Blocked domain names, URLs and IP addresses are referenced in two lists:



- Either you operate a whitelist. Users filtered in this way can only access sites and IP addresses included in the whitelist;
- Either you operate a blacklist. Users filtered in this way can access all sites and IP addresses except those blacklisted.

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.).

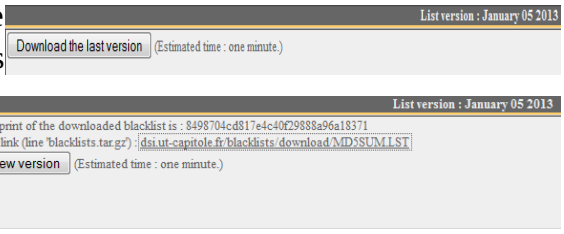
ALCASAR uses **the excellent** list (black + white) drawn up by the University of Toulouse (France). This list was chosen because it is distributed under a free license (creative commons) and its content refers to France. In that list, domain names (e.g., www.domaine.org), URLs (e.g., www.domaine.org/rubrique1/page2.html) and IP addresses (e.g., 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.).

4.1. Blacklist and Whitelist

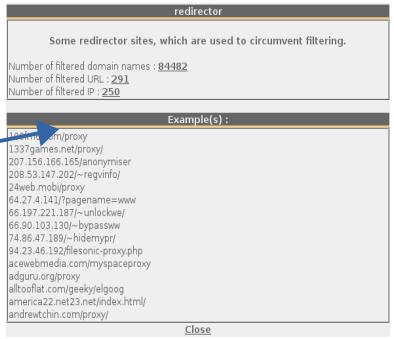
a) Updating the list

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.



b) Editing the blacklist and whitelist

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



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 numbers, you display the first 10 values.

You can rehabilitate domain names or IP addresses.

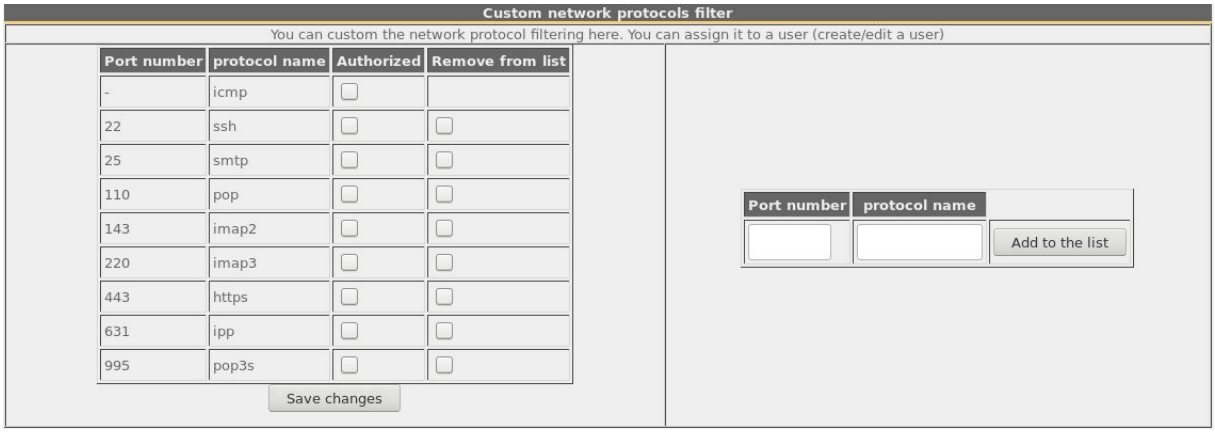
You can add domain names or IP addresses directly in the ACC or by importing text files. These files can be enabled, disabled or removed. Each line of these test files can be a domain name or an IP address.

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.

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

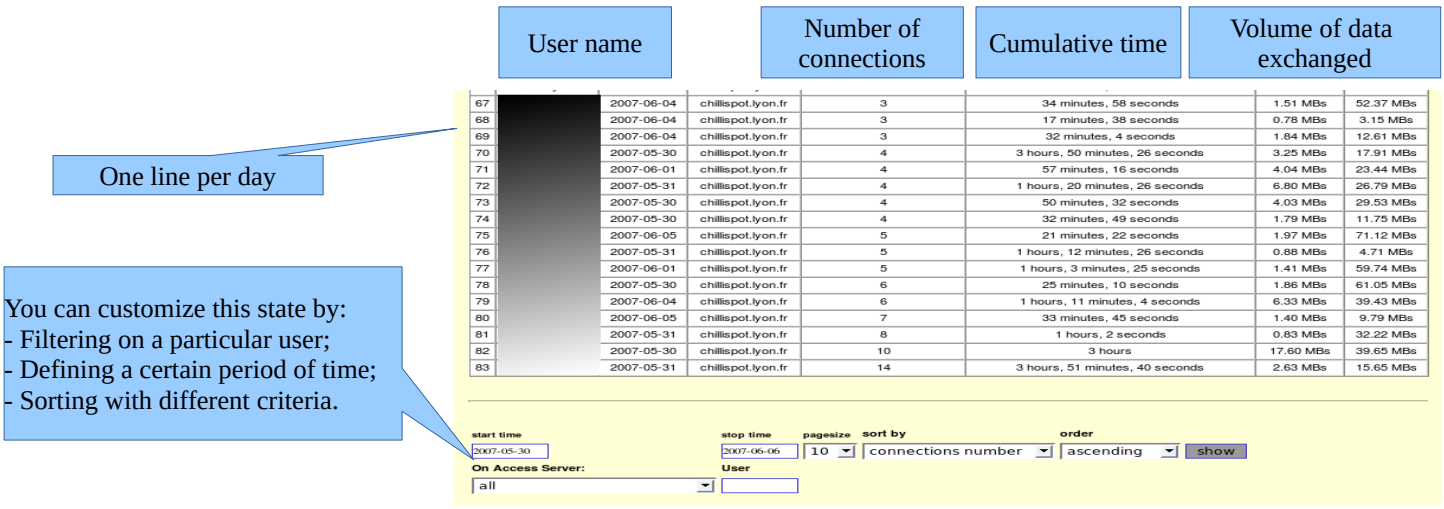
5. Access to Statistics

Statistics 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).

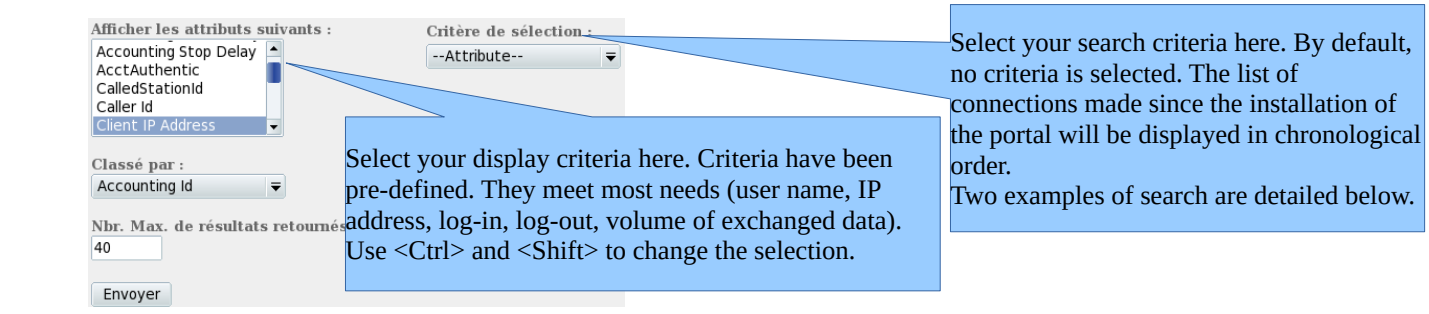
5.1. Number of connections per user per day

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).



5.2. Connection status of users

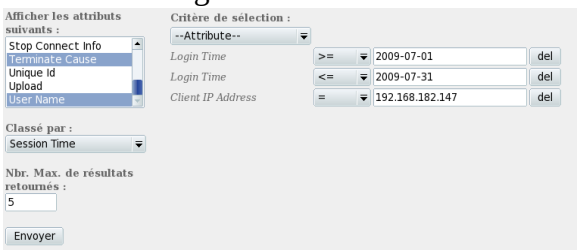
This page lists login and logout events from the portal. An input box allows you to specify your search and display criteria.
With no search criteria, the chronological list of connections is displayed (since the installation of the portal).
Please note: the volume of data exchanged is what ALCASAR sent to the user (upload) or what it received from the user (download).



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

Client IP Address	Download	Login Time	Logout Time	Session Time	Upload	User Name
192.168.182.10	443.61 KBs	2009-05-29 11:19:54	2009-05-29 11:32:34	12 minutes, 40 seconds	11.52 MBs	
192.168.182.22	1.66 MBs	2009-06-03 18:24:20	2009-06-03 18:44:20	20 minutes	33.55 MBs	
192.168.182.129	46.12 MBs	2009-06-03 18:58:23	2009-06-04 09:39:01	14 hours, 40 minutes, 38 seconds	1.10 GBs	
192.168.182.10	381.81 KBs	2009-06-04 12:58:10	2009-06-04 13:06:08	7 minutes, 58 seconds	1.77 MBs	
192.168.182.10	400.14 KBs	2009-06-04 13:41:29	2009-06-04 13:43:45	2 minutes, 16 seconds	1.55 MBs	
192.168.182.10	327.07 KBs	2009-06-04 14:50:24	2009-06-04 15:22:37	32 minutes, 13 seconds	1.29 MBs	
192.168.182.10	96.93 KBs	2009-06-04 15:23:13	2009-06-04 15:37:46	14 minutes, 33 seconds	443.14 KBs	
192.168.182.10	286.75 KBs	2009-06-04 15:38:37	2009-06-04 16:20:42	42 minutes, 5 seconds	375.28 KBs	
192.168.182.129	10.33 MBs	2009-06-04 16:29:46	2009-06-04 19:15:48	2 hours, 46 minutes, 2 seconds	463.62 MBs	
192.168.182.119	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:

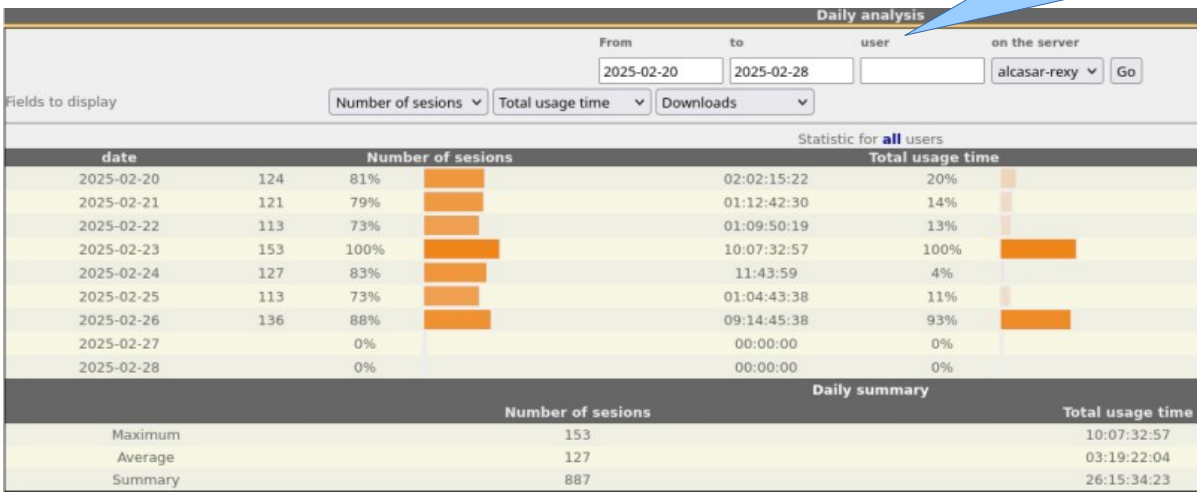


Client IP Address	Login Time	Logout Time	Session Time	Terminate Cause	User Name
192.168.182.147	2009-07-01 14:07:28	2009-07-01 14:08:30	1 minutes, 2 seconds	User-Request	
192.168.182.147	2009-07-21 10:57:19	2009-07-21 10:58:26	1 minutes, 7 seconds	Admin-Reset	
192.168.182.147	2009-07-01 16:21:43	2009-07-01 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).

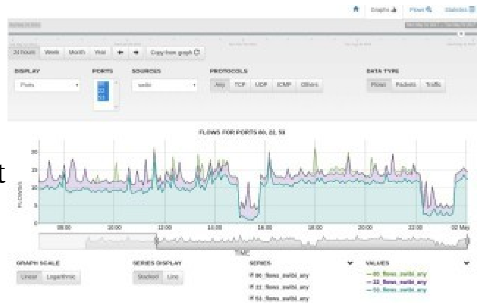


5.4. Global traffic

This graph allows showing network statistics by the hour, day, month.

5.5. Detail traffic

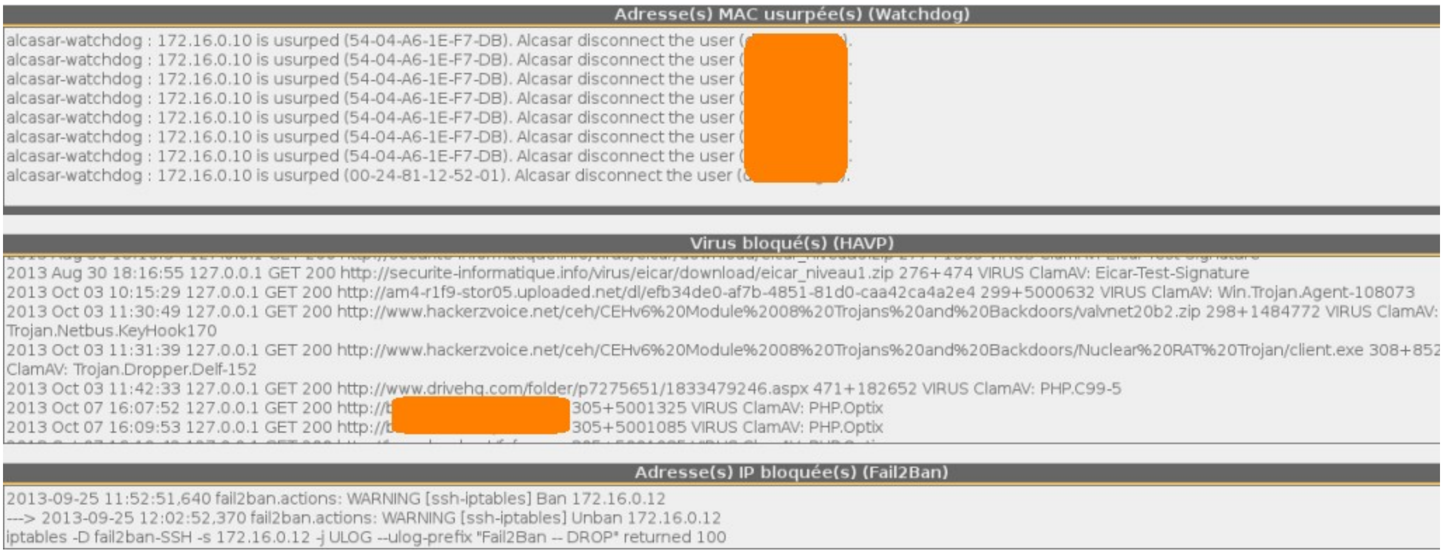
This web page allows searching/showing Netflow traffic (global or by port 22, 53, 80 and 443).



5.6. Security Report

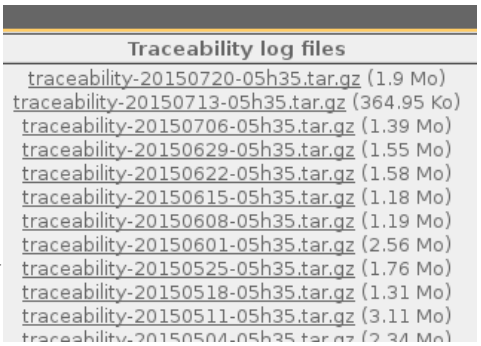
This page displays three safety information identified by ALCASAR:

- The list of users disconnected due to a MAC address spoofing of their device;
- The list of 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.



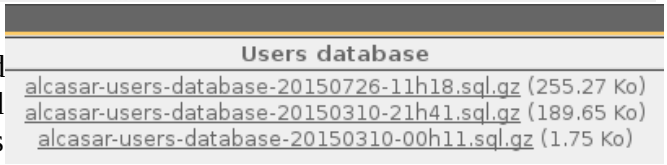
6. Backup

6.1. Connection logs



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.

6.2. The users database



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).

6.3. Weekly activity reports

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

6.4. Accountability logs

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 connection.

⚠ 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
[redacted]	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. Advanced features

7.1. Administrator accounts management

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:

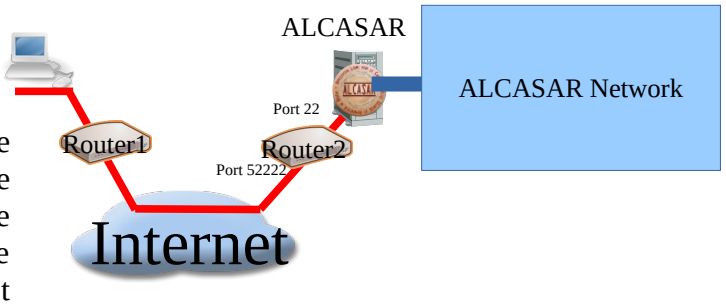
- « admin » : with this profile, the accounts give access to all the functions of the ACC. A first “admin” account was created during the installation of ALCASAR (see Installation documentation);
- « manager »: with this profile, the accounts only gives access to users and groups management functions (see §3) ;
- « backup » : with this profile, the accounts only gives access to backup and archiving of log files (see previous chapter).

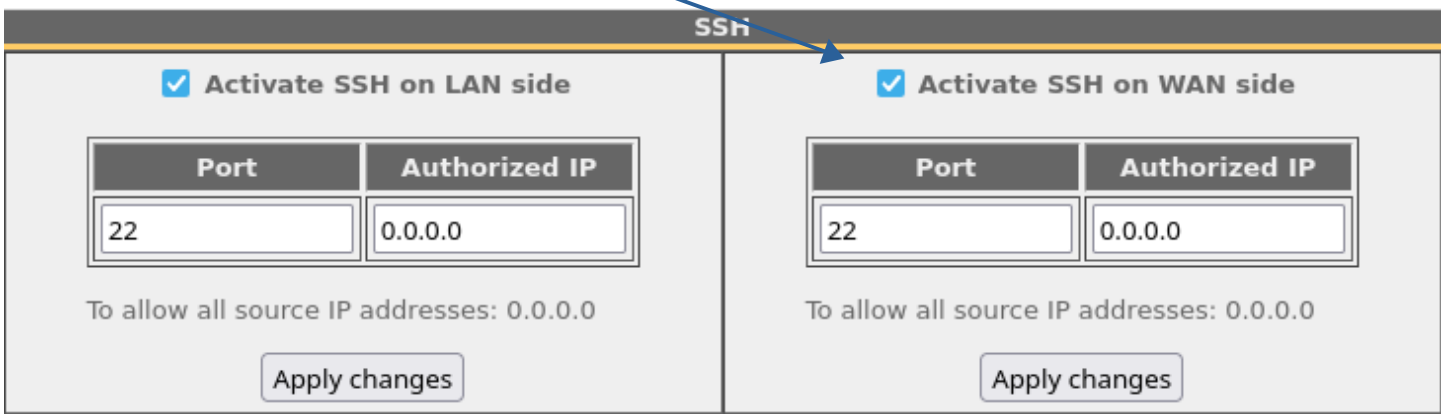
You can create as many administrator accounts as you want in each profile. To manage these management accounts, use the « *alcasar-profil.sh* » command as « root » :

- *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. Secure administration across the Internet

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. First of all, you have to make sure that the "SSH" service on ALCASAR is activated on the Internet side (menu "system", then "network"). You must also know the public IP address of the Box2.





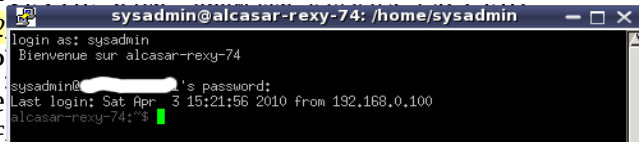
a) Broadband modem/router configuration

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.

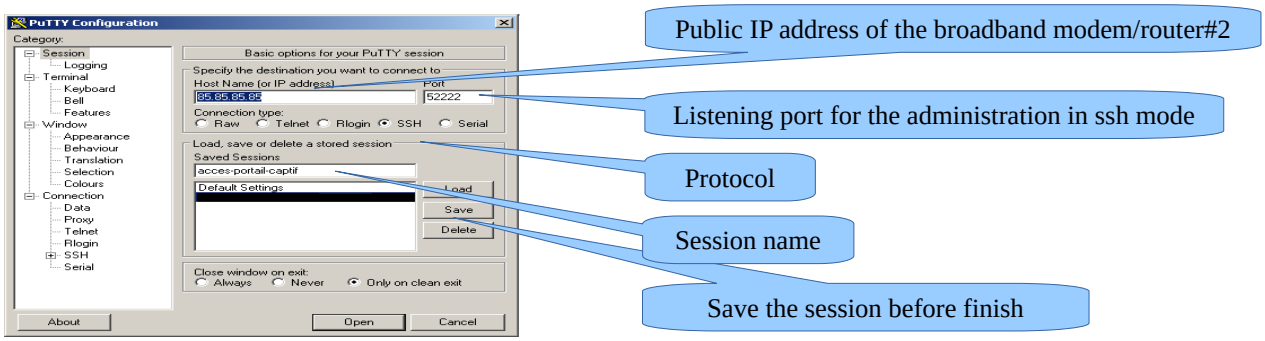
b) administration of ALCASAR in text mode

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 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:

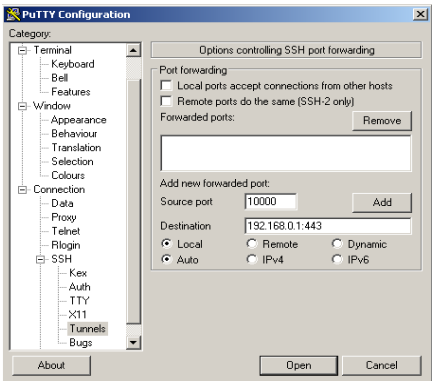


click on "Open", accept the server key and log in as "sysadmin".

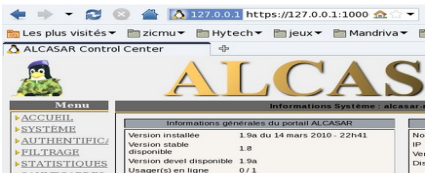
c) Administration ALCASAR in GUI mode

The goal is now to use this SSH connection to graphically administrate the remote ALCASAR. To do that, we redirect the Web browser flow of the administor in the SSH tunnel, and then to the internal card of the remote 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".

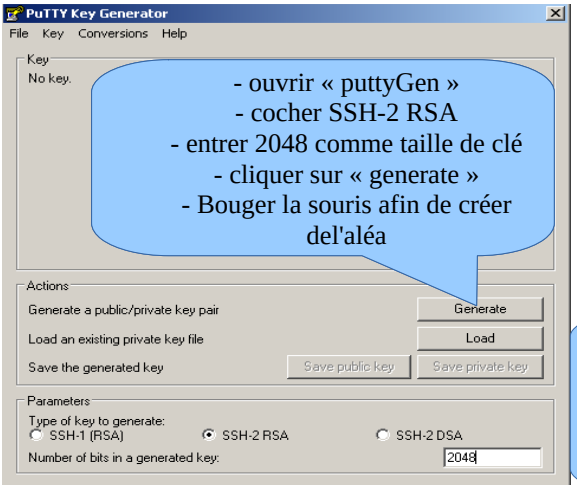
Run the command : *« ssh login@localhost:10000 »* to use SSH for secure remote administration.

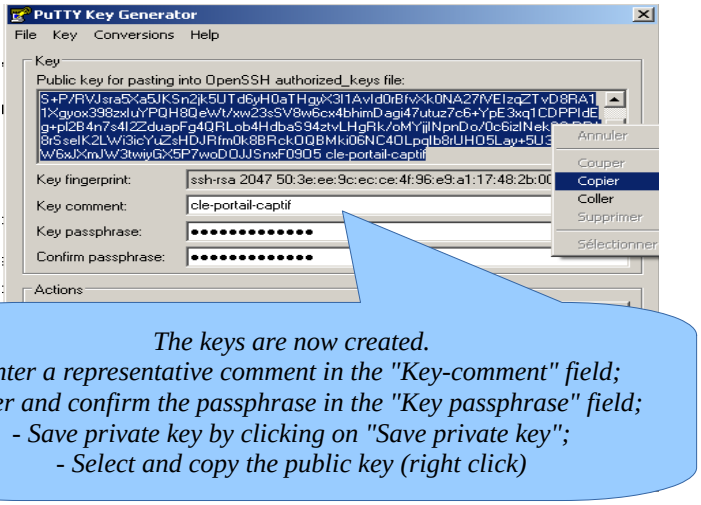
To connect the web-based interface, go to : *« http(s)://localhost :10000 ».*

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.

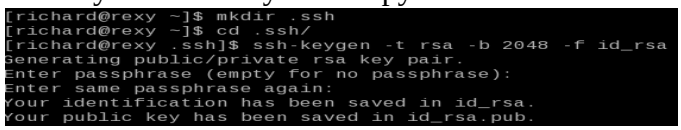
- generate a keys pair (public key / private key)
  - On Windows with « puttygen »

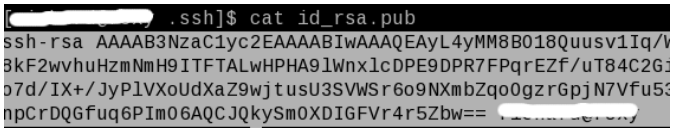




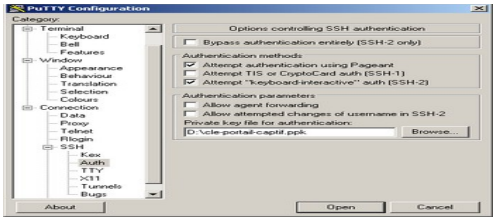
  - Linux with« *ssh-keygen* »

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.

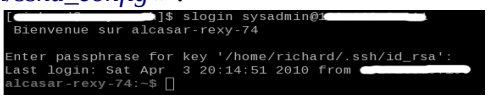




- Copy the public key on the remote portal:
  - run the following command to copy your public key directly on the remote server:
    - *ssh-copy-id -i .ssh/id_rsa.pub sysadmin@<@IP_interne_consultation>*
    - Enter your password; your public key is copied in the *sysadmin/.ssh/authorized_keys* automatically 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* »).

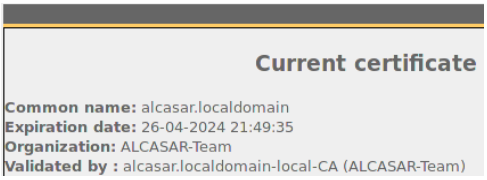
7.3. Display your logo

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. Modifying the certificate of security

Data are 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 “system + network” page of the ACC. If the server certificate is expired, you can regenerate it with the following command : « *alcasar-CA.sh* ».

⚠ 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:

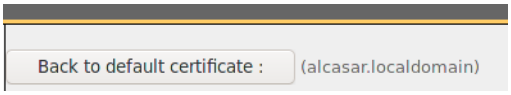
- The private key you used to create the “certificate request” (extension : .key)
- The certificate created by the provider (extension : .crt or .cer)
- Optionally : the file which defines the certification chain of your provider (extension : .pem). When requested, this file is available on the provider website.

Once imported, wait about 1’ for all ALCASAR services will be restarted.
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 restart all the systems connected to the consultation network.
- You can’t use the hostname “alcasar.lan” any more. Use the new hostname instead (“alcasar.rexy.fr” in this example).

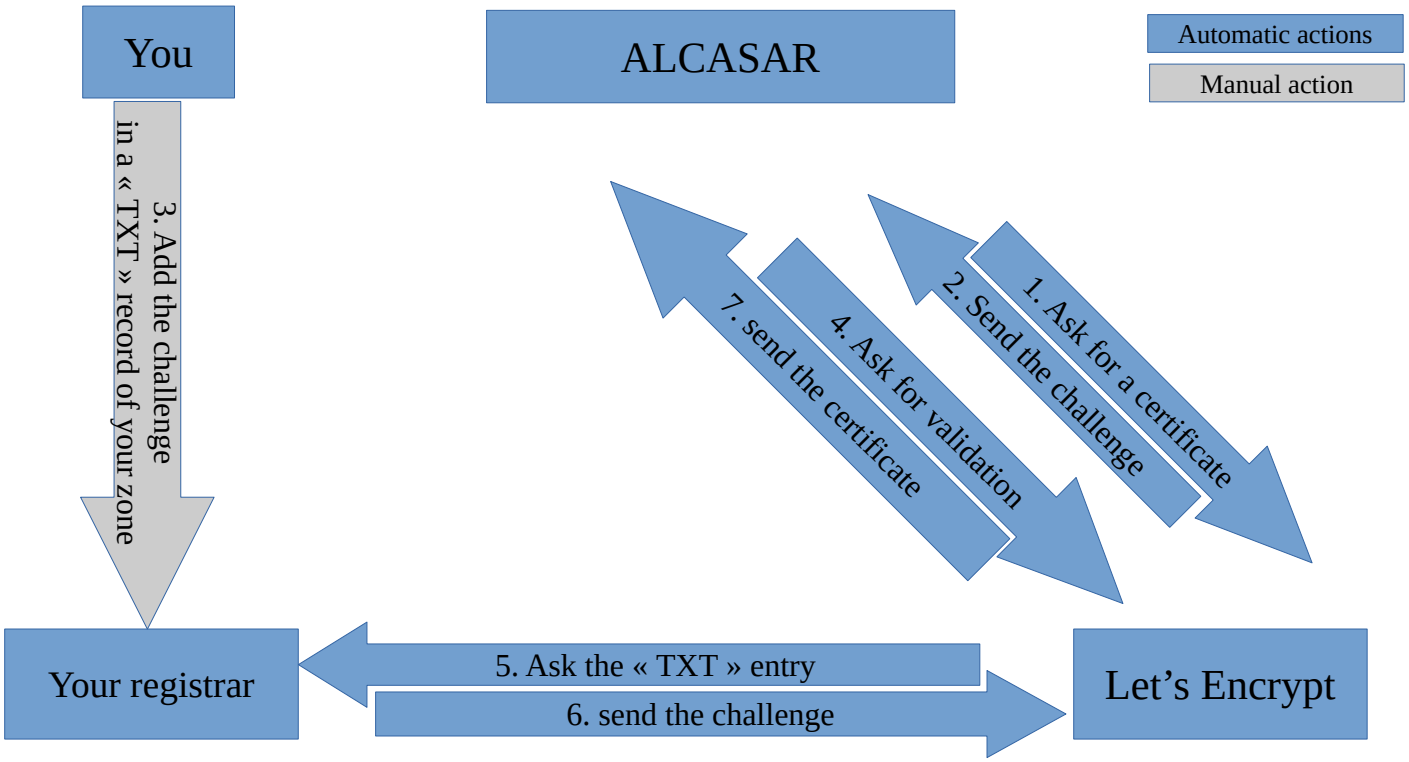
⚠ In case of issues, you can go back to the original auto-signed certificate via ACC or with the command line : « alcasar-importcert.sh -d ».



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 ACC or via the « *alcasar-letsencrypt.sh* » script. Before running these procedures, you must own 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 in 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 these strings. After that, you have to ask "Let's Encrypt" to verify it. Once validated, Let's encrypt send you the certificate. The following scheme shows you the certificate creation process.

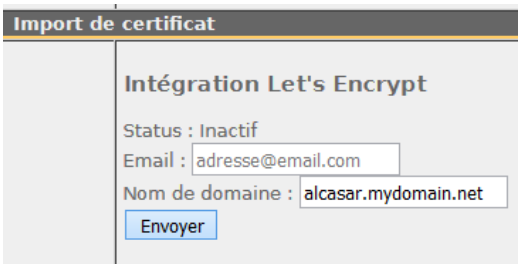


The next paragraph explains how to execute the "Let's Encrypt" certificate request procedure on ALCASAR via ACC or via the command line.

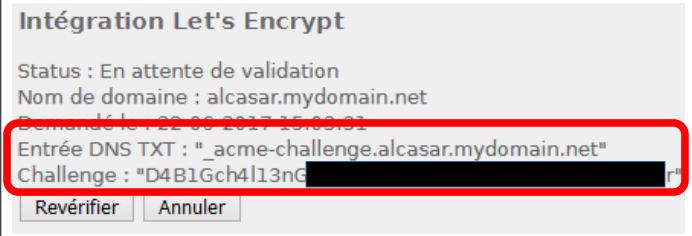
Several DNS providers offer to automate the validation of Let's Encrypt certificates via their API (Application Programming Interface). Appendix §11.4 presents feedback from ALCASAR users who have integrated this possibility.

Via ALCASAR Control Center (ACC)

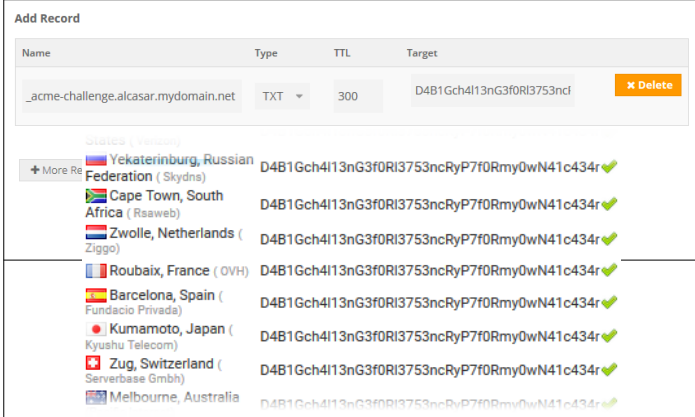
ALCASAR → 1. Ask for a certificate → Let's Encrypt

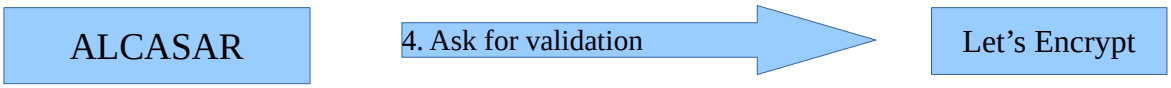
Messages displayed on ACC	Actions
	Write your email address. Write the host name and the domain name of your ALCASAR. Example shown: hostname = "alcasar" and domain name = "mydomain.net".

ALCASAR ← 2. Send the challenge ← Let's Encrypt

Messages displayed on ACC	Actions
	The name and the value of 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".

You → 3. Add the challenge in a DNS « TXT » record → Your registrar

Messages displayed on ACC	Actions
	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.
	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... - dig +short -t TXT _acme-challenge.alcasar....



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 : "D4B1Gch4l13nG[redacted]" Revérifier Annuler	Click on « Verify » to run the validation request to Let's Encrypt. When succeed, Let's Encrypt sends the certificate to ALCASAR which includes it to all processes that need it.
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 it at the expiration date of the certificate.

Once imported :

- You must restart all the systems connected to the consultation network.
- You can't use the hostname "alcasar.localdomain" any more. Use the new hostname instead ("alcasar.mydomain.net" in this example).

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 ».

Via the command line

Creation

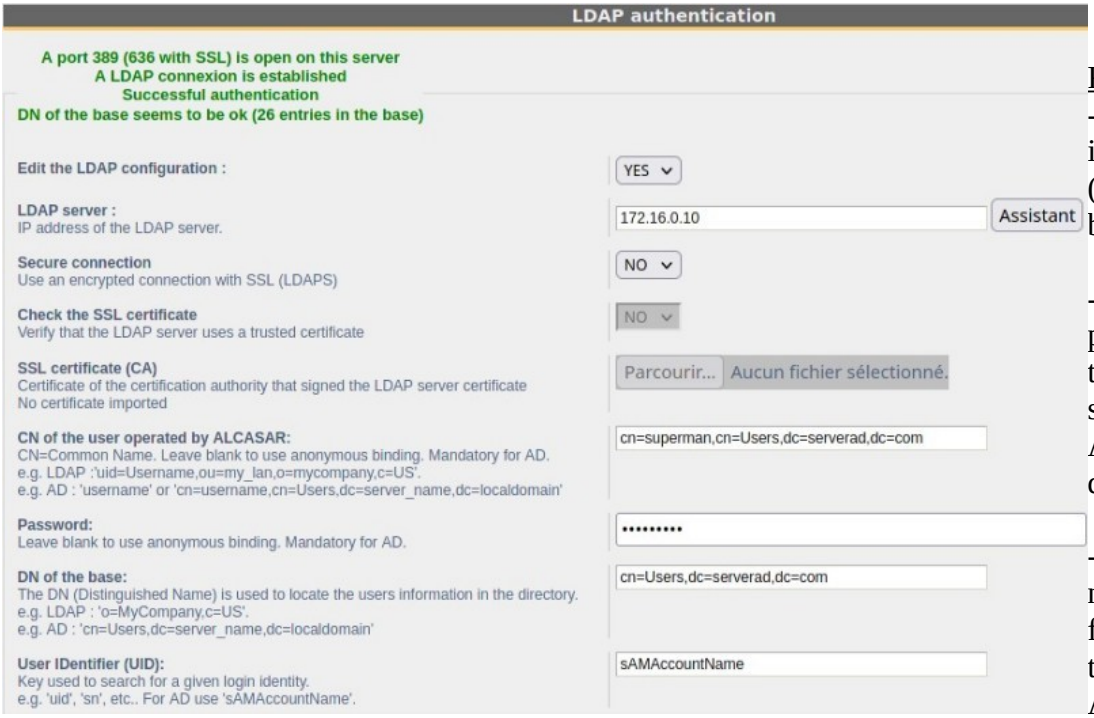
1) Ask a certificate for « alcasar.mydomain.net » :

   « `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).

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

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 :

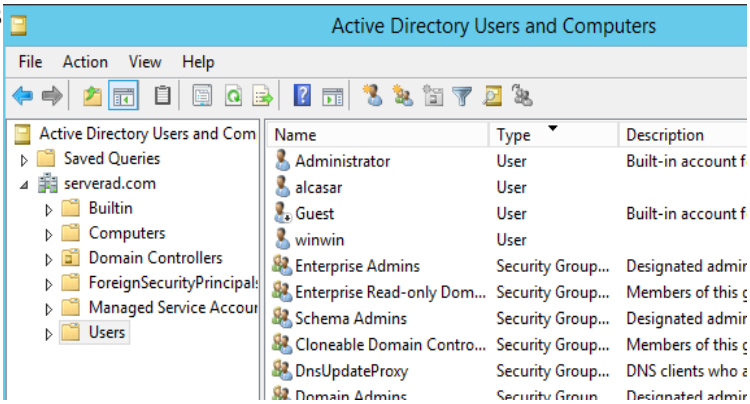


Remark :
- attributes of users stored in the external directory (like the passwords) can't be modified with the ACC;

- if you don't use secured protocole (ldaps), be sure to master the network segment between ALCASAR and the directory server(cf. § 10);

- External directories do not support case sensitive for the login name unlike the local database of ALCASAR.

Examples of an A.D.: 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.



- DN of the base : 'dc=Users,dc=serverad,dc=com'. This DN set the position where searching the users.
- UID : 'sAMAccountName' for an A.D.; 'uid' in general for other LDAP servers.
- User search filter : leave this field empty unless you want to select only specific users.
- User operated by ALCASAR : 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.
- Password : password affected to the user operated by ALCASAR.

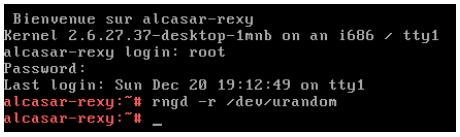
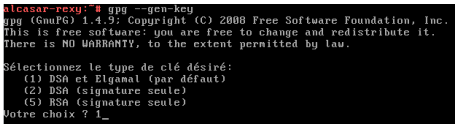
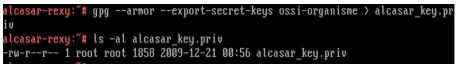
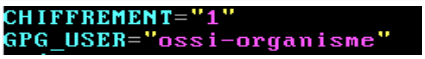
It is possible to provide some specific ALCASAR attributes (bandwidth, concurrent session, etc.) to all the users of an external directory. To do that, create an ALCASAR group named "**ldap**" (in lower case) for which you set the desired attributes.

It is also possible to assign attributes to a particular account authenticated with an external directory. To do this, create an ALCASAR user with the same login name 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. Encryption of log files

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:

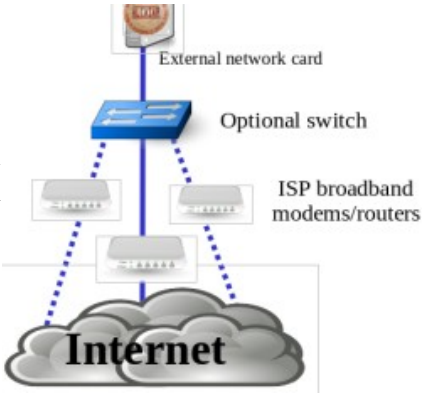
Print screen	Comments	To do
	- Log on as « root ». - Start the entropy generator (random values).	*rngd -r /dev/urandom*
	- Generate the key pair (public key + private key). - Choose the algorithm, the size and the lifetime of the keys (no expiration). - Choose a user name and passphrase.	*gpg --gen-key* info: The user name must not contain spaces. This name is summarized in the term <username> later in this procedure.
	- Stop the entropy generator.	*killall rngd*
	- 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.
	- Delete the previously generated keys - Delete the private key from the GPG keyring	*rm -f alcasar_key.priv* *gpg --delete-secret-key <nom_utilisateur>*
	- 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 »

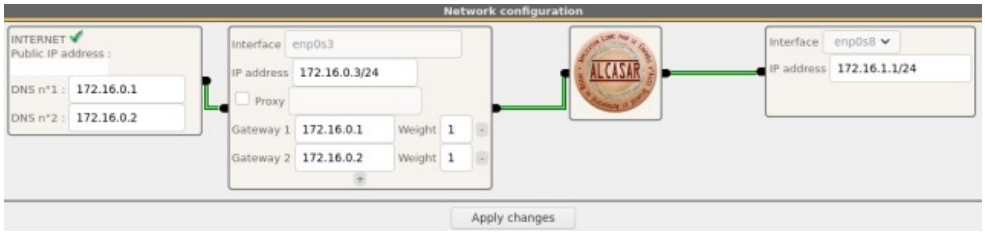
Infos :

- 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 gateways (load balancing)

ALCASAR has a built-in load balancing system when you connect multiple Internet access routers (or gateways). Via the ACC (System + Network), you can add or remove gateways and assign them a "weight". A gateway with a weight of "2" will see twice as much traffic as one with a weight of "1". Load balancing is based on the principle of assigning one gateway per user. You can see this assigment in the menu “authentication” + “activity”.





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 (without fan), low cost and low energy consumption.

An exemple of configuration is the following : 16GB DDR4 - 512GB SSD - **dual RJ45**

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.
Several models under €250 are available under different brands (Nipogi, MinisForum, AceMagic, Sukotop, T9 minipc, Funyet, Trigkey, etc.).

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.

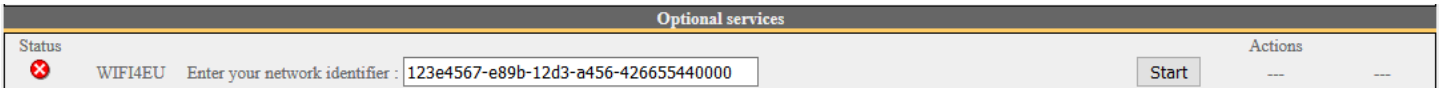
- Bypass the portal by running the script « *alcasar-bypass.sh --on* ».
- To stop it, run the script « *alcasar-bypass.sh --off* ».

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

7.10. WIFI4EU integration

The WiFi4EU initiative promotes free Wi-Fi connectivity for European citizens in public places (parks, squares, public buildings, libraries, health centres, museums, etc.). Municipalities taking advantage of this device must integrate a specific script and the WIFI4EU logo in their access portal. ALCASAR can be modified to integrate this.
The official documentation can be found here : https://ec.europa.eu/inea/en/connecting-europe-facility/cef-telecom/wifi4eu.

In order to operate, you must retrieve your network identifier from the organization that manages "wifi4eu".
You can then activate the service in ALCASAR via the ACC menu : " System + Services ".
The network identifier displayed in the ACC is a test identifier.



When the service is enabled, a "WIFI4EU" logo is inserted at the top of the WEB pages presented to users:

8. Shutdown and update

8.1. Shutdown and restart

There are three possibilities to stop or restart properly the system:

- Via ACC (menu “System” + “Services”)
- by briefly pressing the power button of the PC;
- by connecting to the console as root and running the command "poweroff";

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. Updates

a) Security updates

These updates are performed automatically every night at 03h00.

b) ALCASAR updates

You can perform minor or major updates. In a major update, you must change the version of the operating system (Linux). If the first number of the update (alcasar-**x**.y.z) is different from your running version number, it’s a major update.
You can find out if an update is available by looking at the ALCASAR website, or the front page of the ACC, or by running the command : « *alcasar-version.sh* ».
The following procedure has been created to keep the following settings during the updating process :

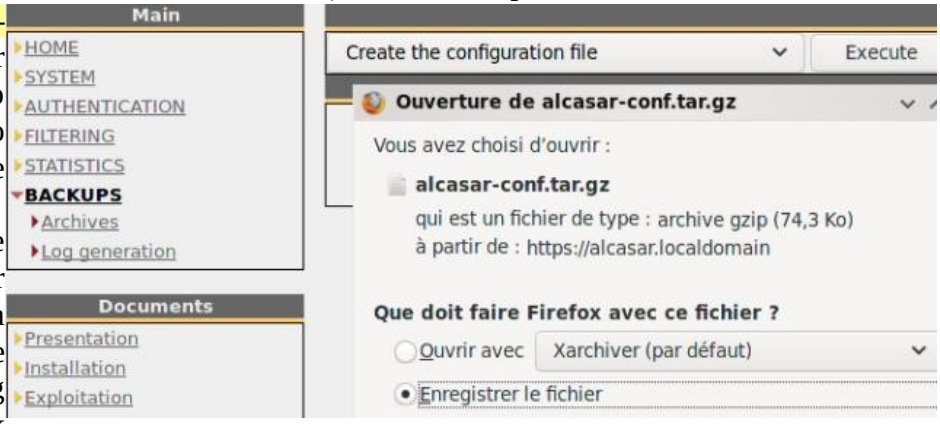
- Network configuration;
- Name and logo of the organization;
- Logins and passwords for ACC administrative accounts;
- Users database (users & groups attributes, connections history);
- Trusted sites;
- Network filtering configuration;
- Certificates of the Certification Authority (C.A.) and the server.

minor updates

Retrieve and uncompress the archive of the version you want. Run the installation script (« *sh alcasar.sh -i* »). It detects your current version and ask you for updating. If the script detects that a minor update is impossible, it informs you to perform a reinstallation (see below).

major update

A major update is needed when a new version of the operating system (Linux) must be installed or when you want to change the hardware (ALCASAR PC).
Via ACC, create a configuration file of the current ALCASAR (menu “Backup” + “Archives” then “create the configuration file”). The file “alcasar-conf.tar.gz” is created in the folder “/var/tmp”. At the same time, it is also available for download. You can also create this file by running the command “alcasar-conf.sh -create”.



If you change the hardware, retrieve this file and copy it in the same folder just before installing the new version of ALCASAR. If you keep the same hardware, install the new operating system keeping the same disk partitionning **without formating the “/var” partition**. Continue with the new installation.

A degraded procedure consists, after installing a new version of ALCASAR, of importing the users base (cf. §3.6a) previously saved (cf. §6.2).

9. Troubleshooting

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. Network connectivity

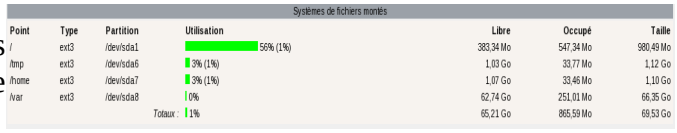
Retrieve the network information in the file "*/usr/local//etc/alcasar.conf*"

- Check the network card status: 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) ;
- gateway/router connection test: 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;
- External DNS servers connection test: Ping the DNS servers. If an error occurs, try with another server;
- Internal DNS server connection test (dnsmasq) : 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* » ;
- Connection test to the Internet: 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;

- Device connection test : 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. Available disk space



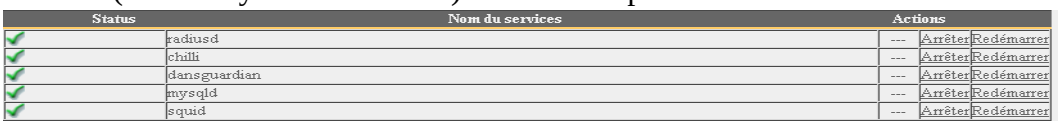
If the available disk space is not enough, some modules may not run properly anymore. You can check the available disk space (especially the */var* partition) :

- in GUI-mode via the homepage of the ACC;
- in text mode, using the command « *df* »

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

9.3. ALCASAR server services

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. Problems experienced

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

a) Windows PC with static addressing

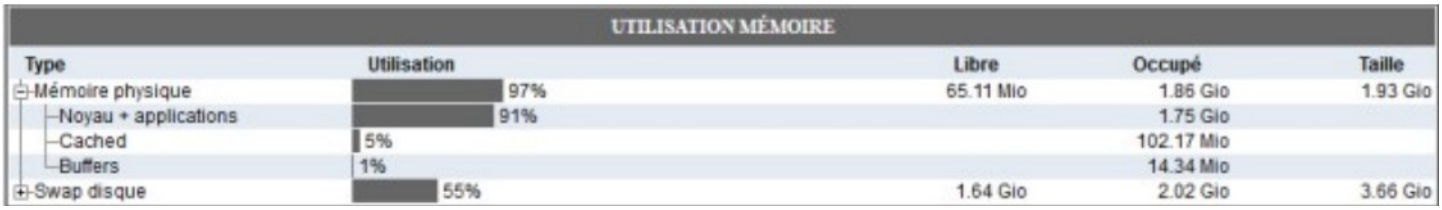
In the DNS configuration of these PC, It is necessary to add the DNS suffix “lan” (Network configuration / Advanced / DNS).

b) 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* ».

c) 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 memory can regularly be beyond 80 percent and can turn red.



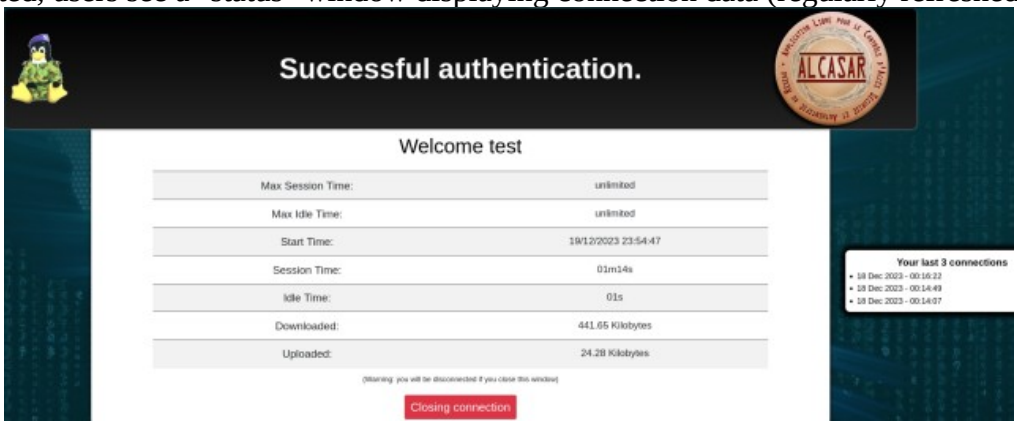
UTILISATION MÉMOIRE

Type	Utilisation	Libre	Occupé	Taille
Mémoire physique	97%	65.11 Mio	1.86 Gio	1.93 Gio
Noyau + applications	91%		1.75 Gio	
Cached	5%		102.17 Mio	
Buffers	1%		14.34 Mio	
Swap disque	55%	1.64 Gio	2.02 Gio	3.66 Gio

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* ».

d) Some users are automatically logged out after 15'

Once authenticated, users see a "status" window displaying connection data (regularly refreshed).



ALCASAR exploits the activity of this window as a "sign of life" for the connected user. On some GSM/tablet devices, when a tab loses focus, it is put to sleep. ALCASAR then disconnects the user, wrongly believing that the user has left the network without logging off.
By setting the "keeping session alive" user attribute to "no", the "status" tab will no longer be considered. Instead, ALCASAR will automatically disconnect the user at midnight, so as not to leave sessions open indefinitely.

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).

10. Security hardening guide

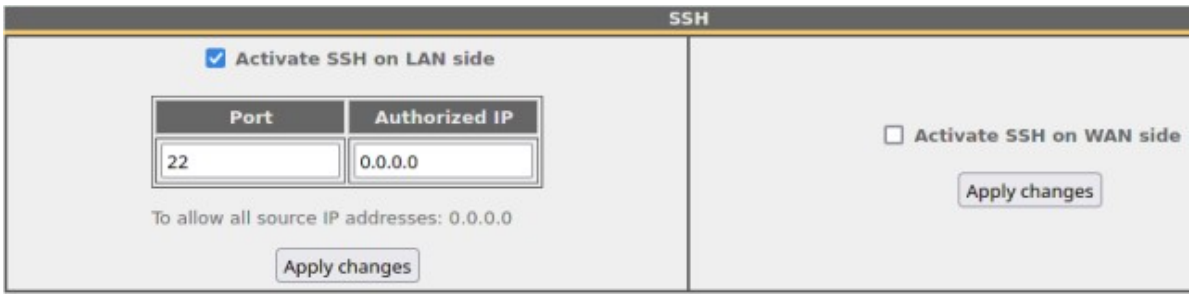
On the consultation network, ALCASAR is the Internet Access Controller. It also helps to protect the network from external threats or from internal usurpation. To this end, it includes :

- protection credentials theft. The authentication flow between devices and ALCASAR users can be 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 preset 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*);
- 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;
- Limit access to the SSH service (ACC: "System" + "Network" menu):
  - On the WAN side, leave disabled if not needed. If necessary, change the default port number and limit access to only one source IP address (the administrator's) ;
  - Apply the same rules on the LAN side.



10.2. On the network

a) Network type "hotspot"

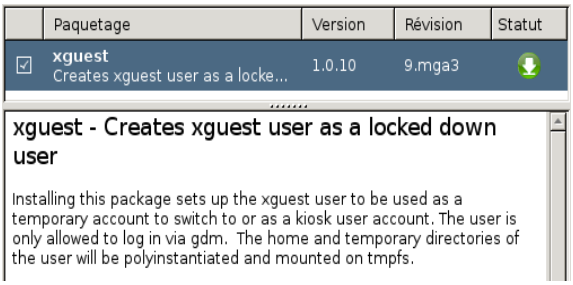
On WIFI Access Points (AP):

- Enable WPA2/3 encryption. It avoids users to listen WIFI traffic.
- 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.

On Ethernet wired switches :

- enable "DHCP snooping" on ALCASAR port and on interswitch ports. This will prevent false (fake) DHCP servers.
- As for the WIFI AP, activate the "client isolation" option.

On the shared consultation equipment:



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 Fedora, RedHat, Mageia and other RPM like 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.*

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 WPA2-3 "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 should/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.lan". The Web server needs to be restarted (*systemctl restart httpd*).
- **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. 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-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 only 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. Helpful authentication exceptions

This chapter presents authentication exceptions that allow devices to access the following services without a user being authenticated:

- licences activation,
- tests of Internet connection,
- Microsoft system update,
- "TrendMicro" 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 : microsoft.com, msftncsi.com et windowsupdate.com*
- *Trendmicro : trendmicro.de et trendmicro.com*
- *McAffee : update.nai.com, akamaiedge.net et akamaitechnologies.com*
- *Clamav : clamav.net*

11.3. Zabbix agent installation

Zabbix is an opensource solution for monitoring systems and networks. This procedure describes the installation of a "zabbix" agent allowing you to monitor ALCASAR servers.
Proposed by Jérôme Gonnot

dowload zabbix agent packet (zabbix-agent 4.0):
wget https://repo.zabbix.com/zabbix/4.0/rhel/7/x86_64/zabbix-agent-4.0.7-1.el7.x86_64.rpm

install the packet ignoring dependencies (libssl et libcrypto):
urpmi --allow-force ./zabbix-agent-4.0.7-1.el7.x86_64.rpm

create the symbolic links:
ln -s /usr/lib64/libcrypto.so.1.0.0 /usr/lib64/libcrypto.so.10
ln -s /usr/lib64/libssl.so.1.0.0 /usr/lib64/libssl.so.10

modify the firewall rules (we use "zabbix" default port):
vim /usr/local/bin/alcasar-iptables.sh
add after line "[INPUT]":
$IPTABLES -A INPUT -p TCP --dport 10050 -j ACCEPT
add after line "[OUTPUT]":
$IPTABLES -A OUTPUT -p TCP --dport 10051 -j ACCEPT
apply the new rules:
bash /usr/local/bin/alcasar-iptables.sh

change the conf file of zabbix agent according to your needs (*/etc/zabbix/zabbix.agentd.conf*).
enable and start the service
systemctl enable zabbix-agent.service
systemctl start zabbix-agent.service

11.4. Automation of let's encrypt validation by DNS Registries

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).

The following link presents a list of DNS registries offering Let's Encrypt validation automation API: https://community.letsencrypt.org/t/dns-providers-who-easily-integrate-with-lets-encrypt-dns-validation/86438/14

a) OVH (by Cédric COULOMB – Merci ;-))

1 - CRÉATION API OVH

Aller sur : https://www.ovh.com/auth/api/createApp
Il faudra s'identifier avec le compte qui gère le nom de domaine pour ALCASAR par exemple alcasar.monsite.fr
Et relever les valeurs - voir ci-dessous : APPLICATION KEY et APPLICATION SECRET
//
Applicaiton name : ALCASAR-COLTEST-3.5.5 (Saisir ce que vous voulez)
Application description : Renouvellement automatique certificat Let's Encrypt pour ALCASAR 3.5.5 (Saisir ce que vous voulez)
APPLICATION KEY : 96xxxxxxexx
APPLICATION SECRET : f99cxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
//

2 - Depuis le serveur ALCASAR en SSH :

Il faudra copier-coller les lignes :
Pour l'Application key (suivant la valeur donnée par OVH)
export OVH_AK="96xxxxxxexx"
Pour l'Application secret (suivant la valeur donnée par OVH)
export OVH_AS="f99cxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx"
acme.sh --issue -d alcasar.monsite.fr --dns dns_ovh
=> Génère une erreur, c'est normal
Créer un compte pour demande de Certificat
acme.sh --register-account -m prenom.nom@monsite.fr
Relancer la commande avec l’option --debug :
acme.sh --issue -d alcasar.monsite.fr --dns dns_ovh --debug
Lire les logs dans la console et relever la ligne pour OVH :
#- => Adding txt value: gnk_E86xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx for domain: _acme-challenge.alcasar.monsite.fr
La valeur "value" sera différente
=> A ajouter dans le DNS de OVH
Vérifier que la modification a bien été diffusée aux principaux DNS avec https://www.whatsmydns.net/ et votre valeur _acme-challenge.alcasar.monsite.fr
Relancer la commande avec l’option --debug :
acme.sh --issue -d alcasar.monsite.fr --dns dns_ovh --debug
Lire les logs dans la console ALCASAR et relever la ligne :
=> validationUrl='https://www.ovh.com/auth/sso/api?credentialToken=xxxxxxxxxxXXXXXXXXXXXxxxxxxxxxxx'
Votre lien sera différent
Suivre le lien puis il faut s’authentifier sur OVH, sélectionner "Unlimited" puis cliquer sur "Authorize Access"
Relancer la commande avec l’option --debug :
acme.sh --issue -d alcasar.monsite.fr --dns dns_ovh --debug

11.5. User sheet

You can provide this form to your users to explain the access control.

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.

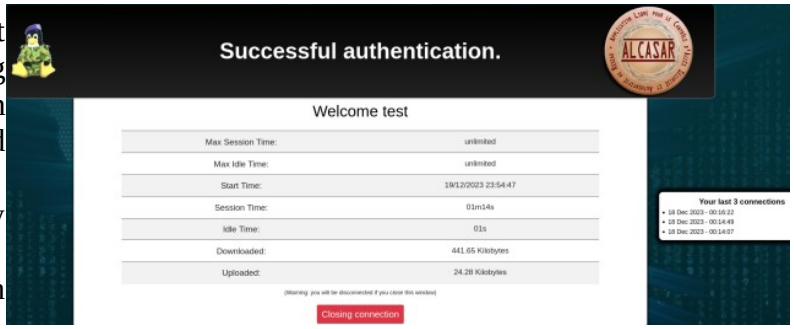
Your WEB browse automatically detect ALCASAR. It should present you a connection bar. If not, connect your Web browser on a **no ciphered** Website (HTTP) like nerverssl.com or euronews.com or on the ALCASAR welcome page (alcasar.lan).
Info : Make sure you have disabled the proxies in your Web browser configuration.

The following window will be displayed.

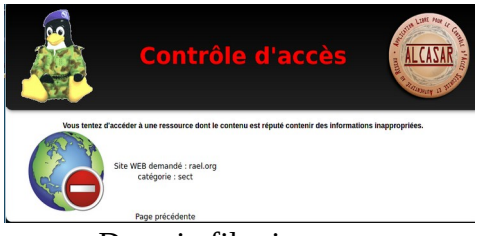
Info: Both fields are case sensitive ("smith" and "Smith" are two different users).

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.lan ».

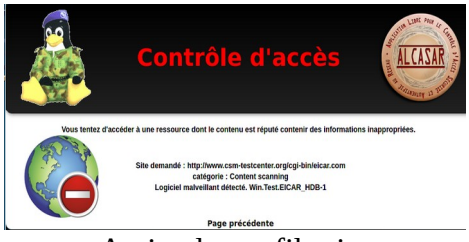
When login is successful, this new tab appears. It allows you to logout from ALCASAR (closing connection). This window provides information on your account permissions (lease time, download limits, connections history, etc.).
If you close this tab, you will be automatically disconnected.
You can also log out with the URL "http://logout" in your browser address bar.



The portal embeds a 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:



Domain filtering



Antimalware filtering

URL filtering