EXPLOITATION

This paper presents ALCASAR exploitation and administration means with the graphical ALCASAR Control Center (A.C.C.) or with Linux command lines.

Project : ALCASAR	Author : Rexy and 3abtux with support of « ALCASAR Team »
Object : Exploitation	Version : 2.7
Keywords : captive portal, access control, accountability, traceability, authentication	Date : 2013 February

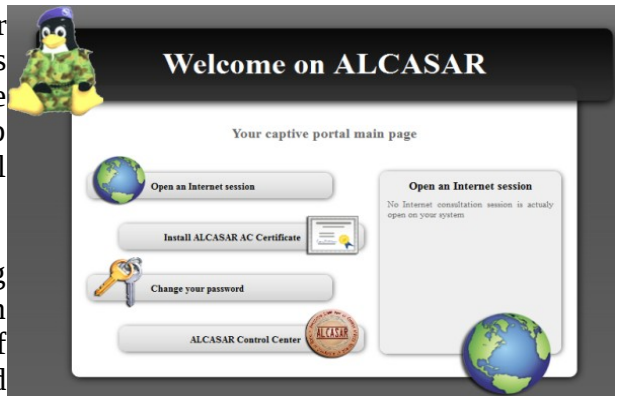
Table of contents

1. Introduction 3
2. Network configuration 4
   2.1. ALCASAR parameters 5
   2.2. Consultation equipment parameters 5
3. Manage equipment 7
4. Manage users 7
   4.1. Users group creation 7
   4.2. Edit and remove group 8
   4.3. Create a user 9
   4.4. Search and edit users 9
   4.5. Import users 10
   4.6. Empty the users database 11
   4.7. Authentication exceptions 11
5. Filtering 12
   5.1. Filter domain names, URLs, and the results of search engines 12
   5.2. Filter network flows 13
   5.3. Exceptions to the filter 13
6. Access to Statistics 13
   6.1. Number of connections per user per day 14
   6.2. Connection status of users 14
   6.3. Daily use 15
   6.4. Consultation WEB 15
   6.5. Firewall 15
7. Backup connection traces 16
   7.1. Logs firewall 16
   7.2. The users database 16
   7.3. If Judicial Inquiry 16
8. advanced Features 16
   8.1. Account Management Administration 16
   8.2. administration through secure Internet 17
   8.3. Implementation of the organization's logo 20
   8.4. Manipulation with the server certificate 20
   8.5. Using an external directory server (LDAP or AD) 21
   8.6. Integration in a complex architecture (AD, DHCP external) 21
   8.7. Encryption of log files 22
   8.8. Load balancing connection 23
   8.9. Create a dedicated housing ALCASAR 23
   8.10. Bypass the portal 23
9. Stop updates and resettlement 24
   9.1. Shutdown 24
   9.2. Updates of the operating system 24
   9.3. Update ALCASAR 24
   9.4. Replacing a portal 24
10. Diagnostics 25
   10.1. Network connectivity 25
   10.2. Available disk space 25
   10.3. Services server ALCASAR 25
   10.4. Connectivity equipment consultation 26
   10.5. Connection to ALCASAR with a serial terminal 26
   10.6. Problems experienced 27
11. Secure 28
   11.1. On ALCASAR 28
   11.2. The consultation network 28
12. Annexes 30
   12.1. Useful commands and files 30
   12.2. Exceptions authentication helpful 31
   12.3. Sheet of User 32

1. Introduction

ALCASAR is an authenticated and secured captive portal. This paper explains how to use and administer it.

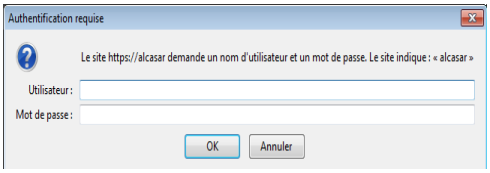
The portal welcome page is available for any WEB browser connected on the consultation network. The URL is http://alcasar. It allows users to connect, to disconnect, to change their password and to load the security certificate into their web browsers. It allows administrators to access to the graphical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

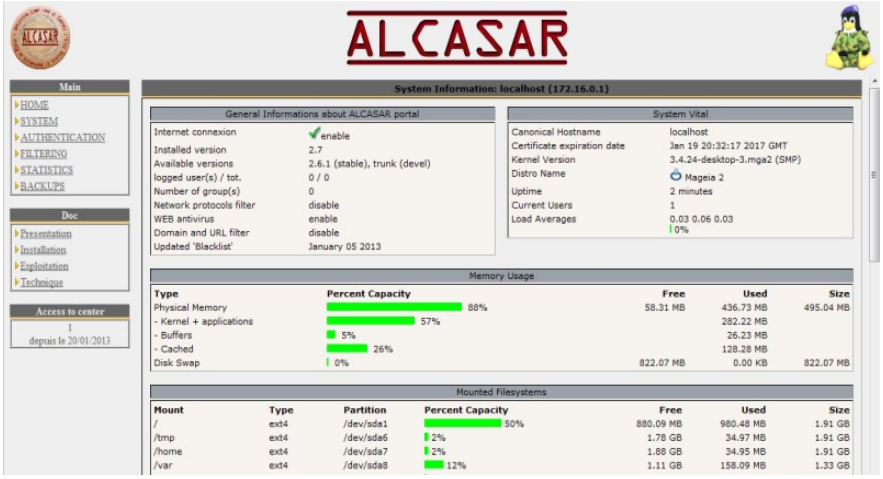


For users conected on the consultation network, the following intercept page is displayed when their WEB browser tries to join an Internet WEB site. This intercept page is displayed in one of 6 languages (English, Spanish, German, Dutch, French and Portuguese) depending of browsers preferences. Until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

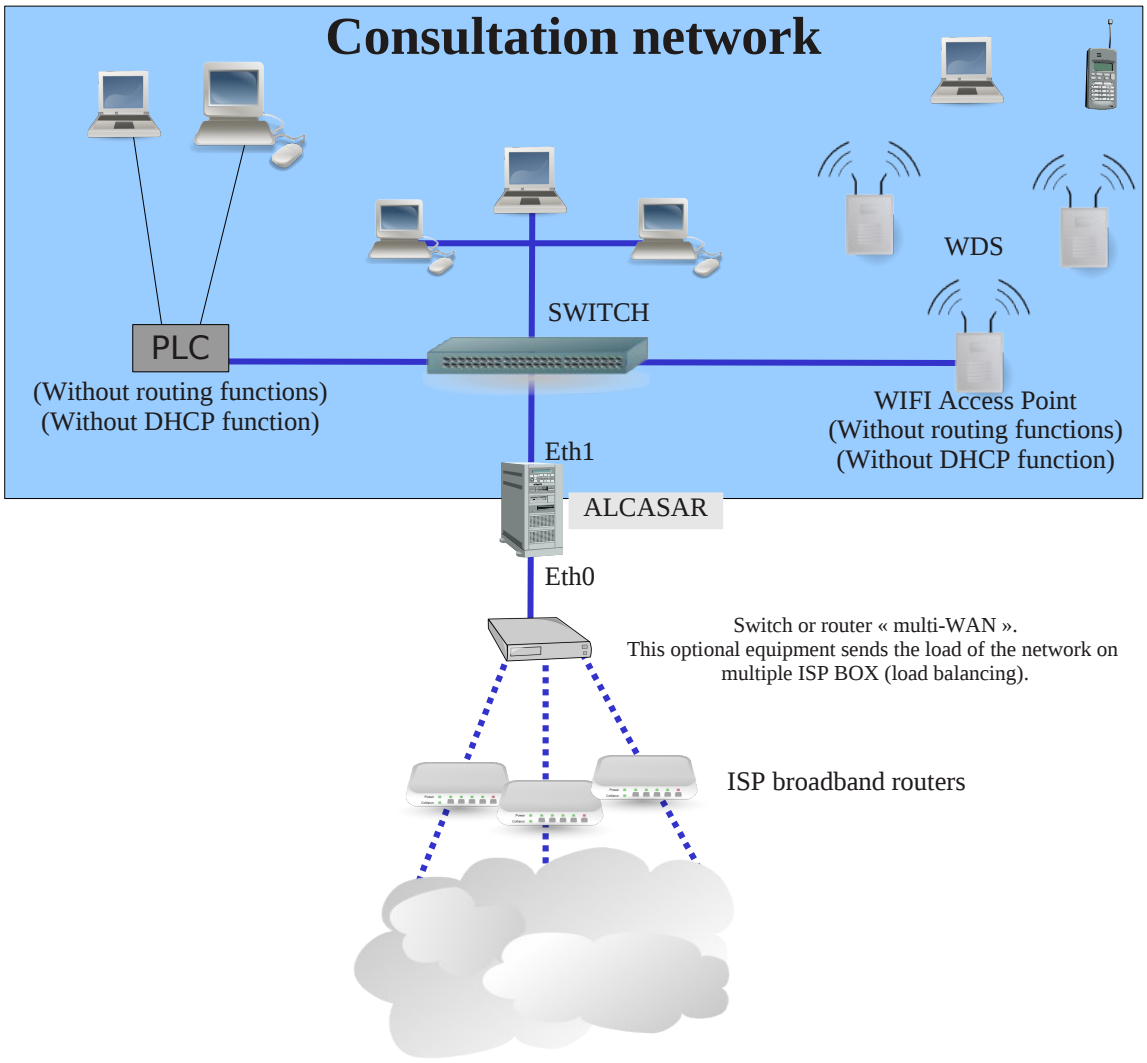
For administrators, ACC is available in a cipher way (https) in two languages (English and French). After succeeding of the authentication process, the ACC is displayed in one of the three following profiles (cf. §7.1) :

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





2. Network configuration



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

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

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

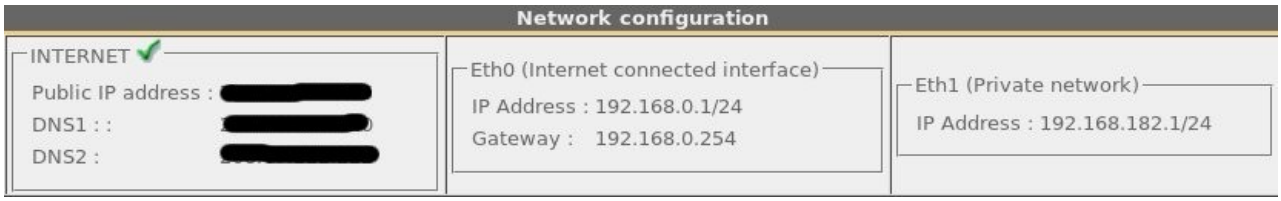
Example of a class C consultation network (default configuration)

- Network IP Address : 192.168.182.0/24 (sub-net mask : 255.255.255.0) ;
- Max number of equipments : 253 ;
- ALCASAR eth1 IP address : 192.168.182.1/24 ;
- Parameters of connected equipments :
  - available IP addresses : between 192.168.182.2 and 192.168.182.254 (statics or dynamics) ;
  - DNS server address : 192.168.182.1 (ALCASAR IP address) ;
  - DNS suffix : localdomain (this DNS suffix must be set in the configuration of static address equipments) ;
  - Default gateway IP address : 192.168.182.1 (ALCASAR IP address) ;
  - network mask : 255.255.255.0

2.1. ALCASAR parameters

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

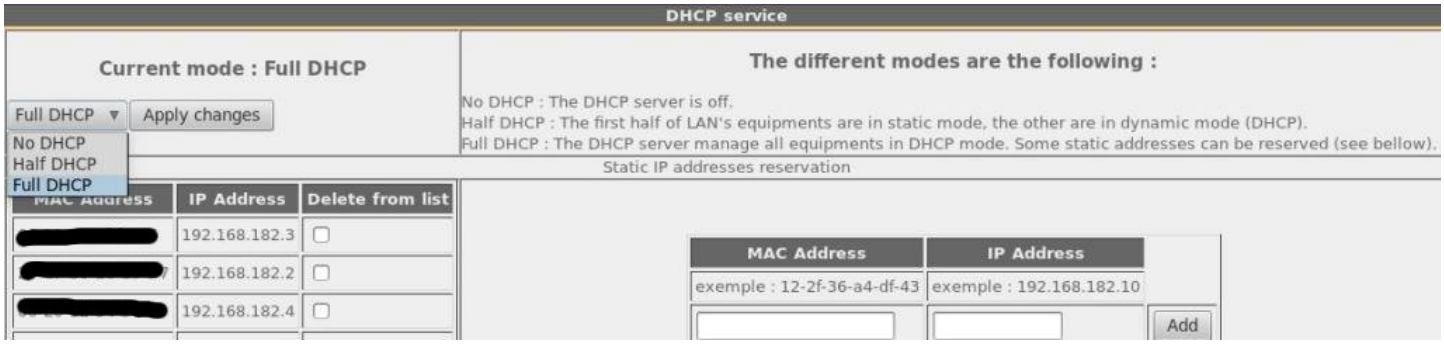
a) IP configuration



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

b) DHCP server

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



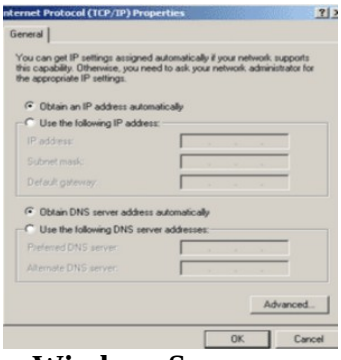
When this service is on, you can reserve IP addresses for equipment that need static IP addresses (servers, printers, WIFI Access Point).
When this service is on, be sure that no other DHCP server is connected on your network (or be sure to well knowing how manage multi-DHCP service (cf. §8.5a to manage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

2.2. Consultation equipment parameters

An explanation sheet for users is available at the end of this paper.
The users only need a simple WEB browser accepting **« JavaScript » and « pop-up » windows**. To be intercepted by ALCASAR, the web browser must point to an Internet WEB site (default start page). The **proxy** parameters must be **disabled** or not be active when Internet surfing through ALCASAR portal.

a) Network configuration

Dynamic address configuration (private user equipment) :



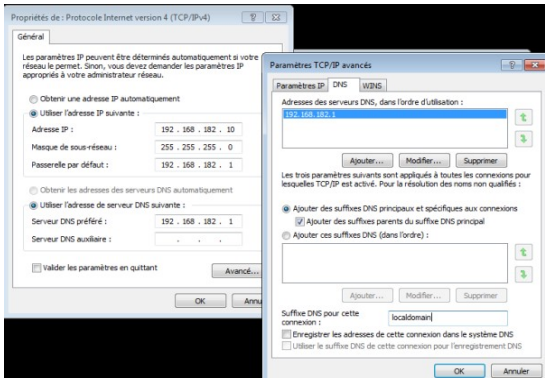
« Windows Seven »

« Mandriva & Mageia Linux »

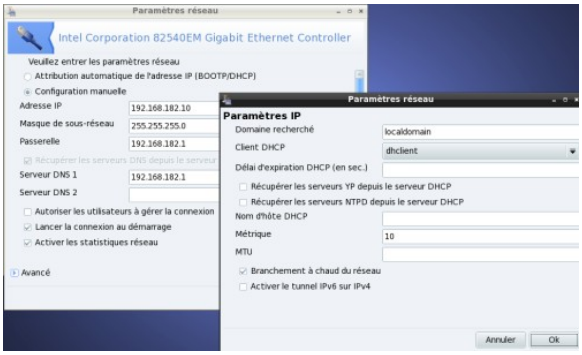
Static address configuration (servers, printers, WIFI access points, etc.) :

For these equipment, the parameters must be :

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



« Windows Seven »



« Mandriva & Mageia Linux »

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

b) Add bookmark

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

c) Incorporate the ALCASAR security certificate

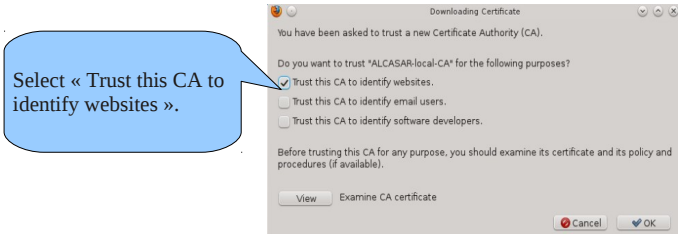
Some communications between consultation equipment and ALCASAR are encrypted with SSL (Secure Socket Layer) protocol. This protocol need two certificates created during the installation process : the ALCASAR certificate and the Local Certification Authority (C.A.) certificate. By default, the WEB browsers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

« Mozilla-Firefox »

« Microsoft-I.E. »

« Google-chrome »

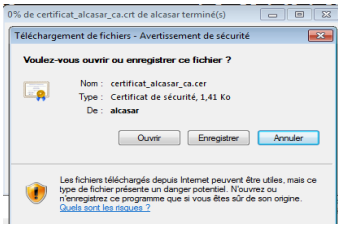
Although is it possible to surf, it's interesting to install the security certificate of this C.A. in browsers in order they don't show these alert windows[1]. To do that, click the zone « Install the root certificate » of the portal main page (« http://alcasar »). For each web browser, follow the following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



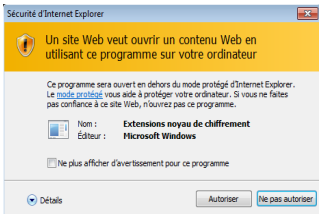
« Mozilla-Firefox »

Konqueror

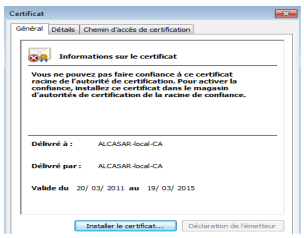
1 You can avoid this manipulation either in buying and including in ALCASAR an official certificate which is known by all web browsers (see §8.4), or in disabling the encryption of authenticating flow via the script « alcasar-https.sh {--on|--off} ». Disabling the encryption of authentication flow implies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



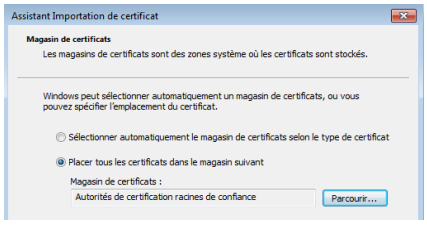
1 – click « open »



2 – click « authorize »



3 – click « install the certificate »



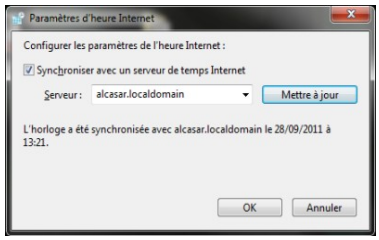
4 – choisissez le magasin « autorité de certification racine de confiance »

« Internet Explorer 8 » et « Safari »

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

d) Time synchronization

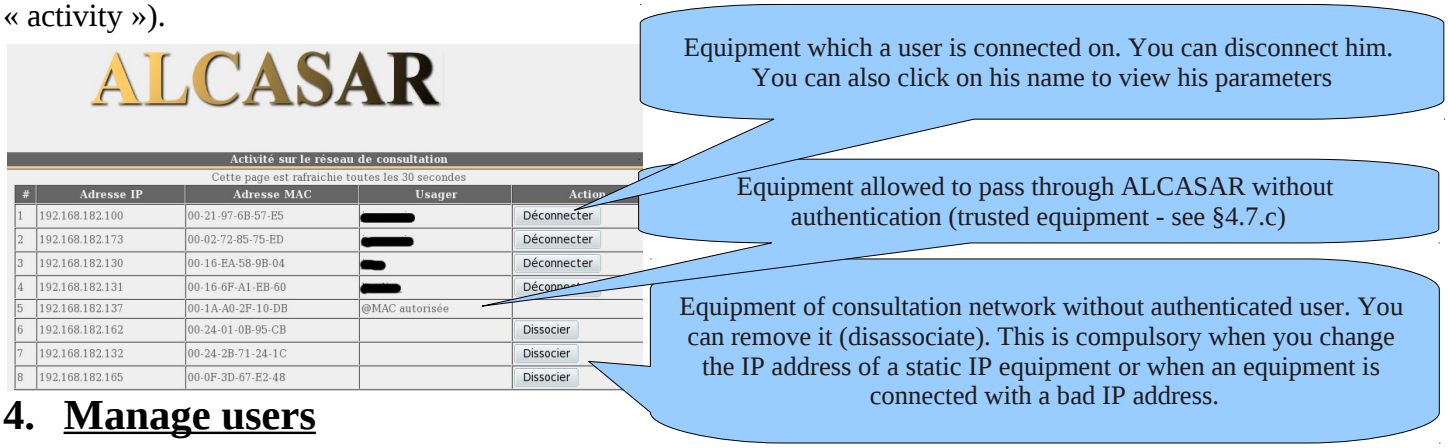
ALCASAR includes a network time server (« NTP » protocol) allow you to synchronize equipment connected on the consultation network. Thus, on Windows or on Linux, you can define ALCASAR as the time server by right clicking on the clock of the desktop. Write « alcasar » on Linux and « alcasar.localdomain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



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

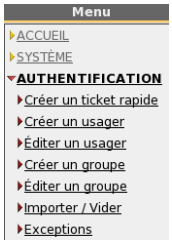
3. Manage equipment

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



4. Manage users

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



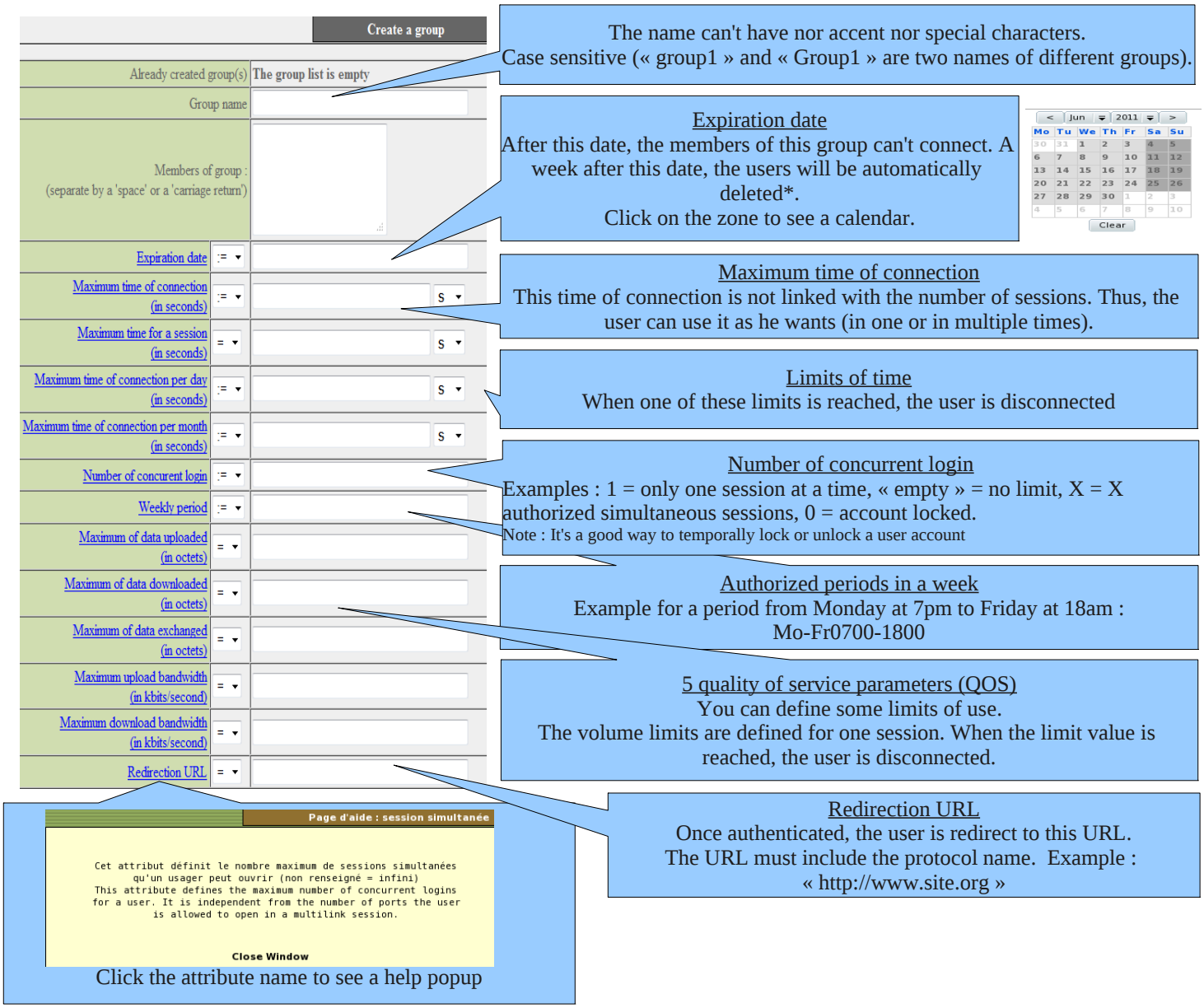
- create, search, modify and remove users or group of users ;
- create a quick ticket (voucher). Only main attributes are shown and are already configured (example : the expiration date is fixed to the day after) ;
- import user names via a text file or via an users database backup file ;
- empty the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

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

4.1. Users group creation

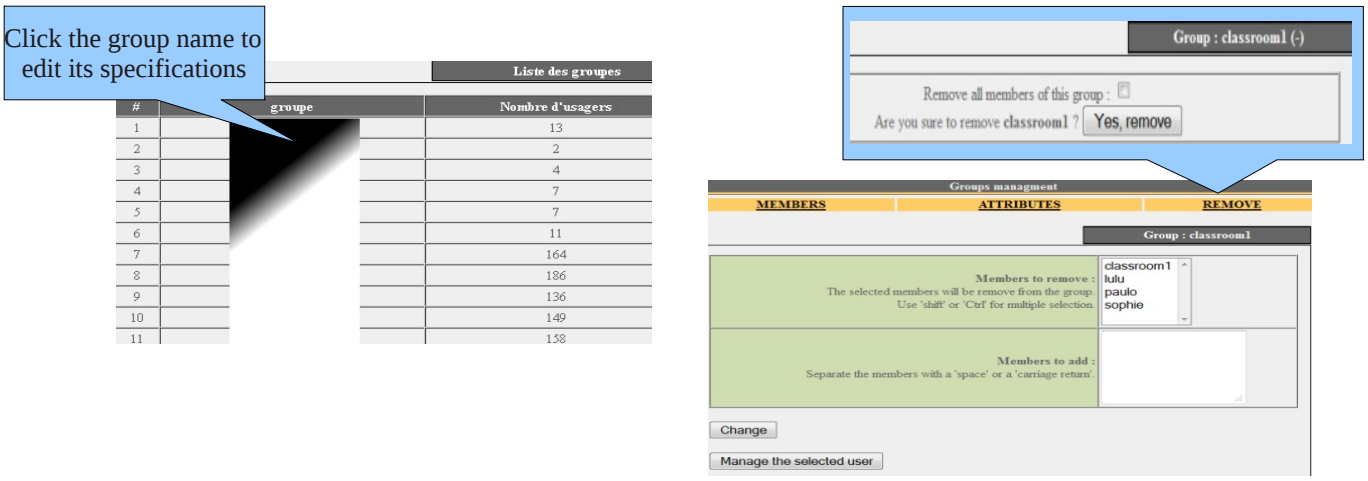
When you create a group of users, you can define the attributes of all the users of this group. These attributes are enabled only if they are not empty. Thus, let the attribute empty, if you don't want to use it. Click the

attribute name to see a help popup.



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

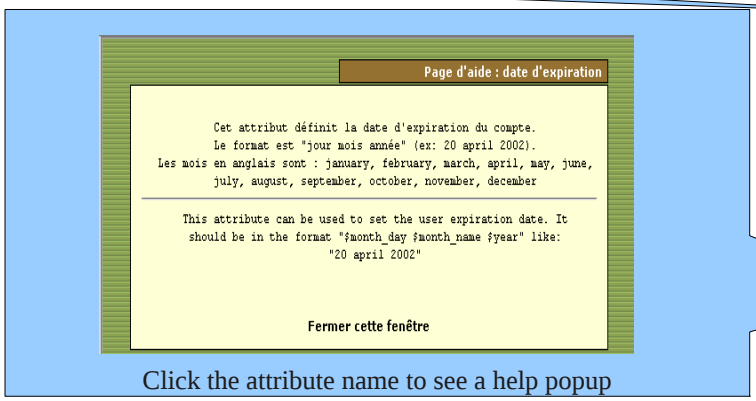
4.2. Edit and remove group



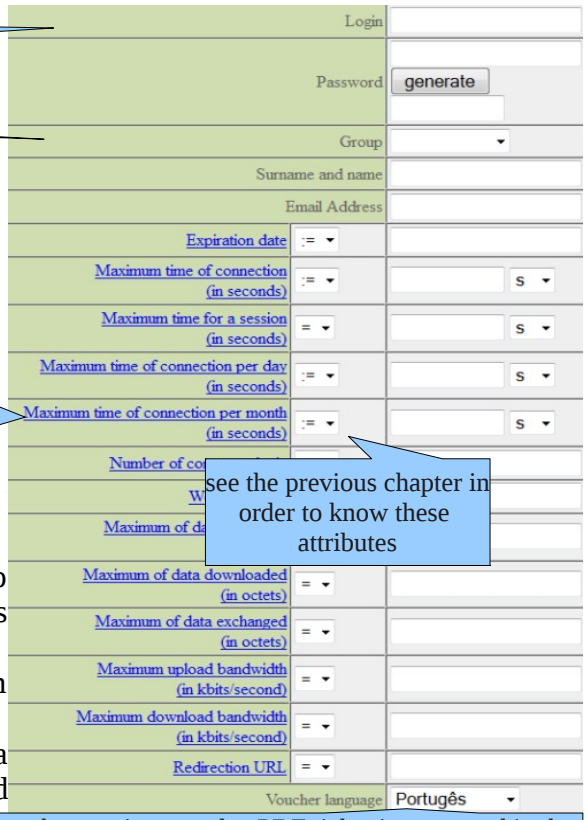
4.3. Create a user

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

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



Click the attribute name to see a help popup



see the previous chapter in order to know these attributes

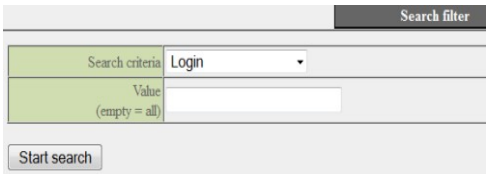
* When an attribute is defined both for the user and for its group (example : maximum time for a session), the user attribute is considered.
* When a user is member of several groups, the choice of the main group is performed in the user attribute window (see next §).
* When a user is locked by one of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

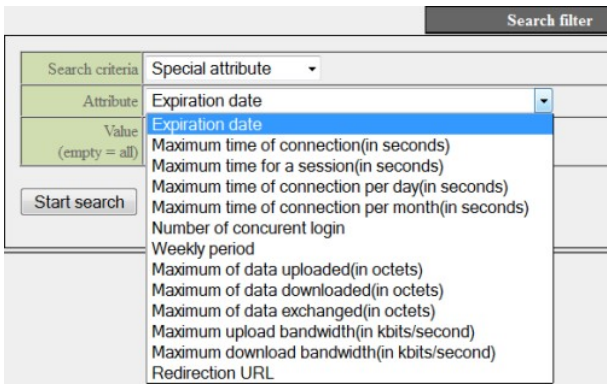
When the user is created, a PDF ticket is generated in the language of your choice.

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

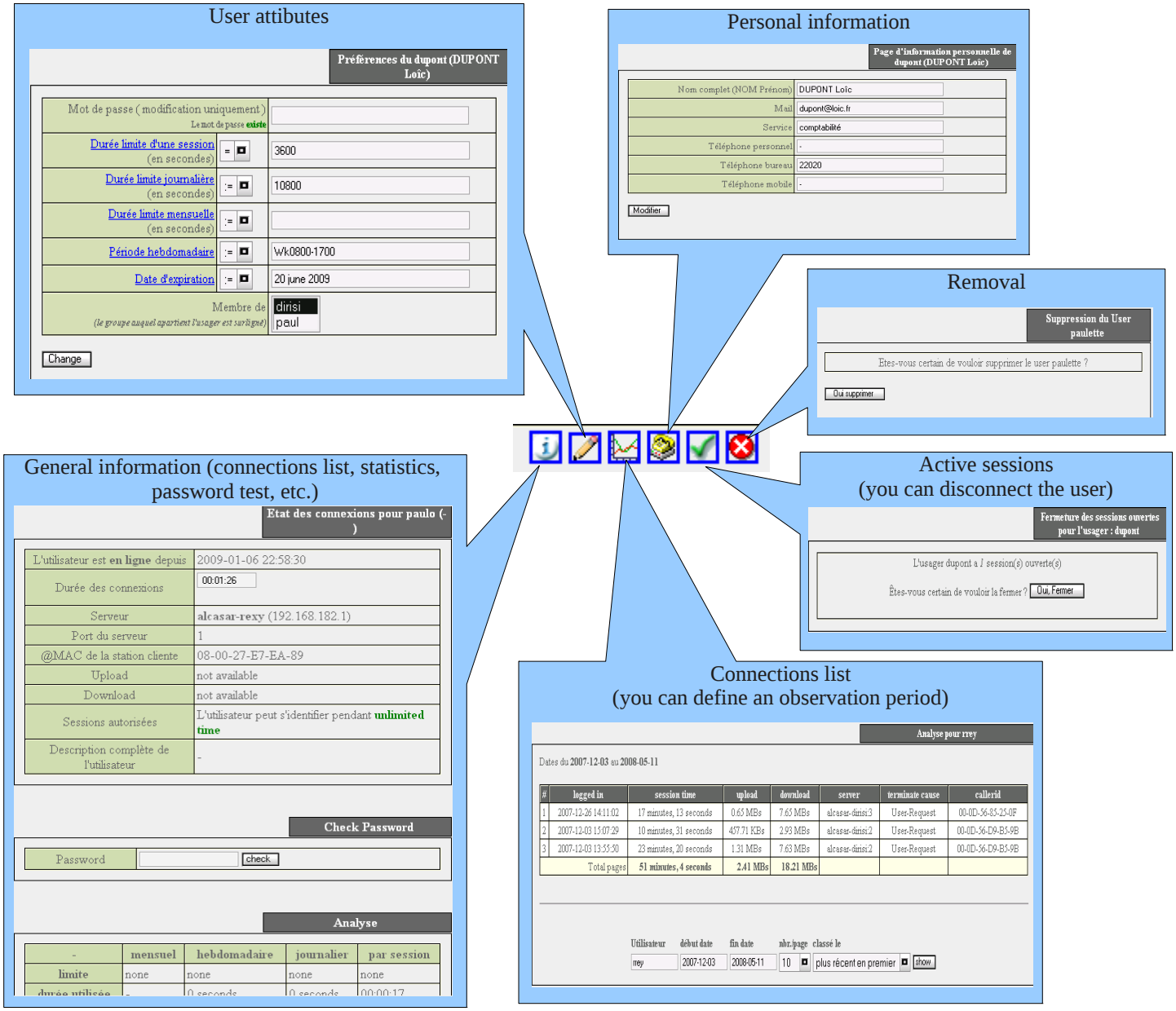
4.4. Search and edit users

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





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

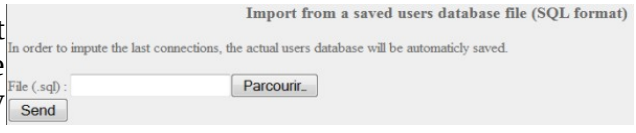


4.5. Import users

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

a) From a backup of users database

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

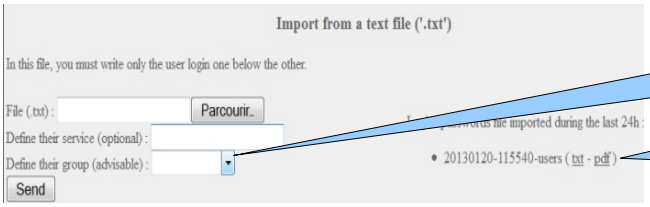


b) From a text file (.txt)

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

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

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



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

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

4.6. Empty the users database

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

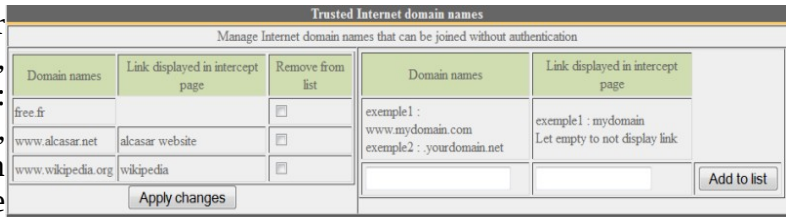
4.7. Authentication exceptions

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

- allow antivirus softwares (and operating systems) to update themselves automatically on the Internet editor sites ;
- access without authentication a server or a security zone (DMZ) situated behind ALCASAR ;
- allow some equipment not to be intercepted ;
- allow the recording of the Seven licenses on the Microsoft site ;
- keep the Windows icon *"Internet access" on*, even if nobody is connected.

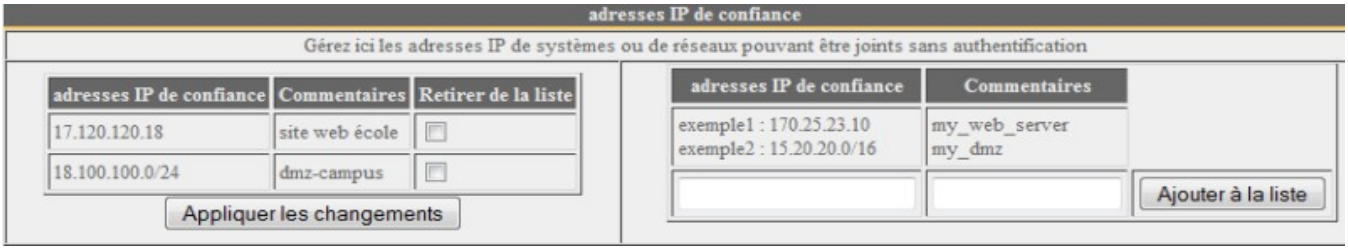
See §12.2

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



In this window, you declare trusted site names or trusted domain names. In case of a domain name, all the linked sites are allowed (example : « .free.fr » allows "ftp.free.fr", "www.free.fr", etc.). You can display the link of a trusted site on the ALCASAR interception page. If you have enabled the protocols filtering (see § 5.2.c), the filter rules are applied on these trusted sites or trusted domain names.

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



In this window, you represent IP addresses or network equipment (for example DMZ). The protocol filtering (see § 5.2.c) has no effect on the addresses reported here.

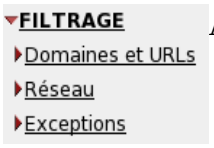
c) Allow equipment trust consultation

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

Having said equipment trust, ungroup it via the menu "System" + "Activity" that consideration be immediate.

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

5. Filtering



ALCASAR has three optional devices filter:

- a filter domain names, URLs and search engine results;
- a stream filter network for blocking some network protocols;
- antivirus on the flow WEB.

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

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

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

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

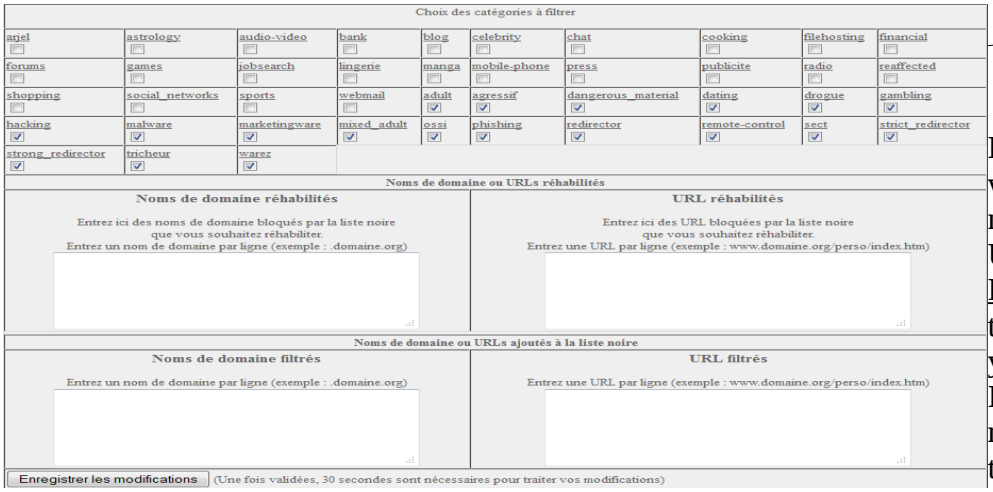
a) Enable and disable filtering

b) Update the blacklist

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

c) Modify the blacklist

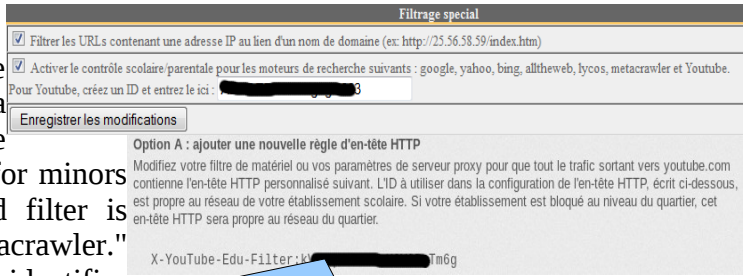
You can choose to filter categories. You can restore or add sites to the« blacklist ».



By clicking on the category name will display its definition and the number of domain names and URLs it contains.
Features: The "ossi" corresponds to domain names and URLs that you add to the blacklist.
Info: if you test screening and rehabilitation, consider clearing the cache browsers.

d) Special filtering

Two special filters are available in this menu. The first block URLs containing an IP address instead of a domain name. The second allows you to exclude the results of search engines links may not be suitable for minors (function "safesearch"). ALCASAR in this second filter is compatible with "Google", "Yahoo", "bing" and "metacrawler."
This filter can work with 'YouTube' long to get an identifier



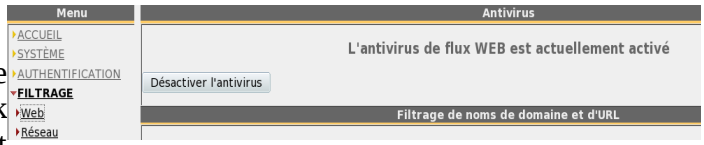
When creating your account "Youtube" Recover your username (string characters located after the ':').

(ID) on YouTube as follows: http://www.youtube.com/education_signup. Once your YouTube account is created, copy the identifier assigned to you in the management interface ALCASAR and save the changes.

5.2. Filter network flows

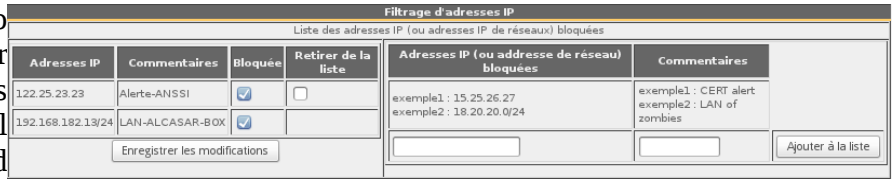
ALCASAR includes a filter module to allow only network flows deemed necessary.

a) Antimalware flow WEB



ALCASAR operates free product "clamav" to analyze and filter the flow of web pages within the network consultation. It is enabled by default and filters out viruses and spyware (keyloggers, adware). Update its knowledge base is performed automatically every two hours. You can test its operation in attempting to retrieve a test file located at the URL: http://eicar.org/anti_virus_test_file.htm

b) IP address filtering or network address



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

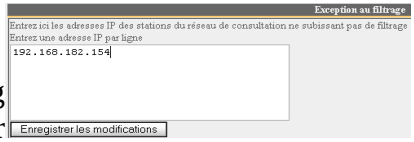
c) Filtering protocols

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

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

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

5.3. Exceptions to the filter



Menu "exception" to define the IP addresses of network undergoing consultation or network filtering or filtering domain name and URL filtering or search engines (facilities management staff, to adults, teachers, etc.).. The filter remains active malware.

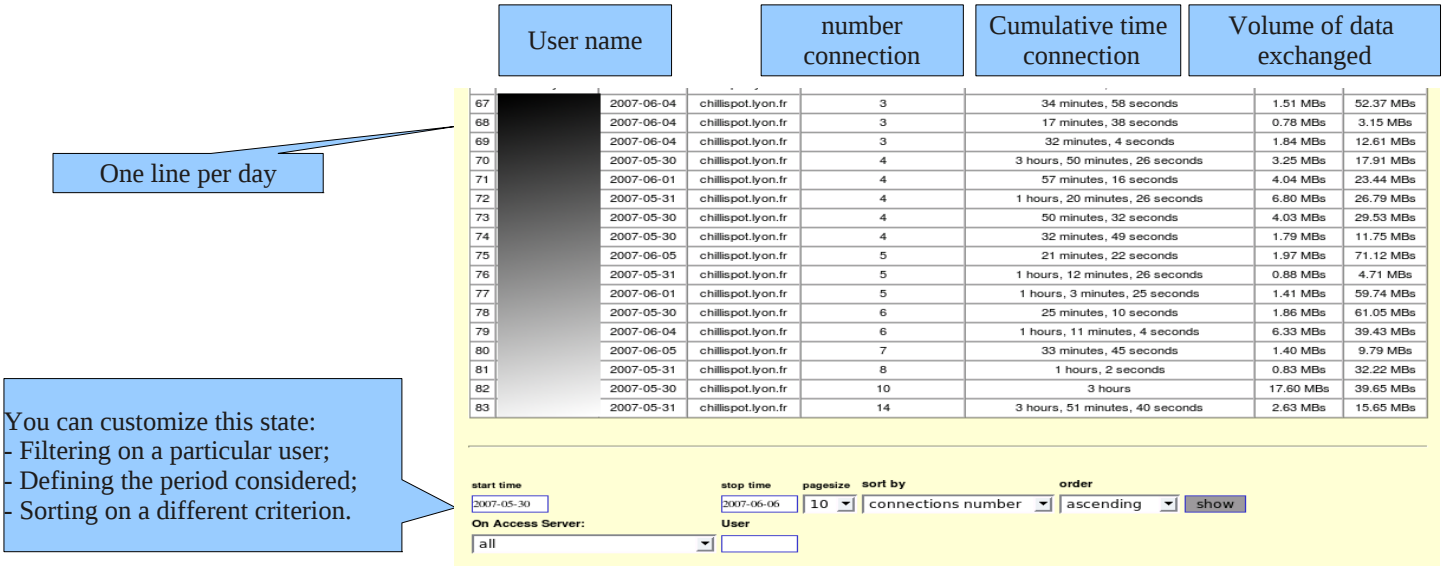
6. Access to Statistics

The interface statistics are available, after authentication, the management portal page (menu "statistics." This interface provides access to the following information:

- number of connections per user per day (update every night at midnight);
- connection status of users (updated in real time);
- daily load of the portal (updated every night at midnight);
- statistical consultation WEB (updated every 30 minutes);
- reaction firewall (updated in real time).

6.1. Number of connections per user per day

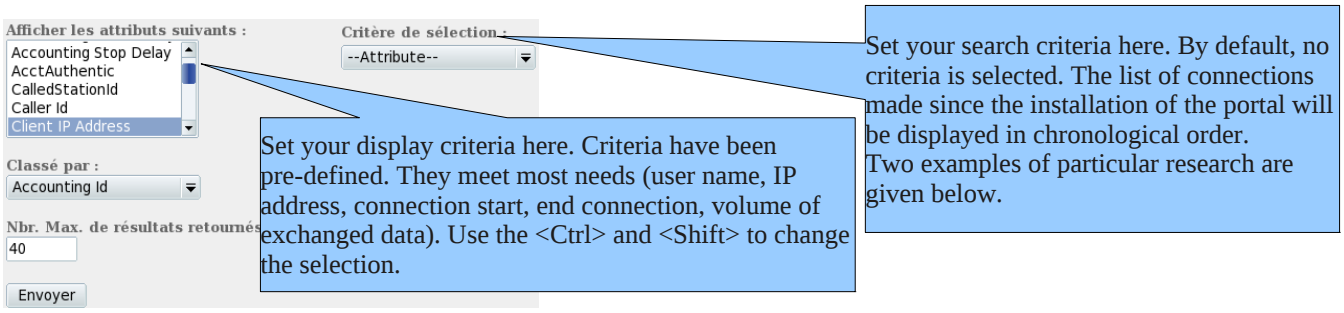
This page displays per day per user, the number and connection time and data volumes exchanged. Warning: the volume of data exchanged corresponds to ALCASAR sent to the user (upload) or receive user (download).



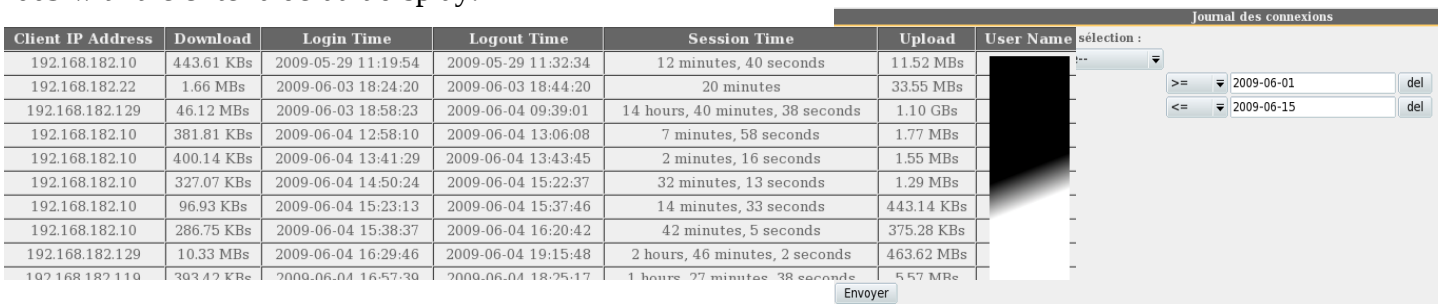
67	[redacted]	2007-06-04	chillispot.lyon.fr	3	34 minutes, 58 seconds	1.51 MBs	52.37 MBs
68		2007-06-04	chillispot.lyon.fr	3	17 minutes, 38 seconds	0.78 MBs	3.15 MBs
69		2007-06-04	chillispot.lyon.fr	3	32 minutes, 4 seconds	1.84 MBs	12.61 MBs
70		2007-05-30	chillispot.lyon.fr	4	3 hours, 50 minutes, 26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

6.2. Connection status of users

This page will list the opening and closing session performed on the portal. An input box allows you to specify your search and display criteria.
Regardless of particular research, chronological list of connections is displayed (since the installation of the captive portal). Warning: the volume of data exchanged corresponds to ALCASAR sent to the user (upload) or receive user (download).

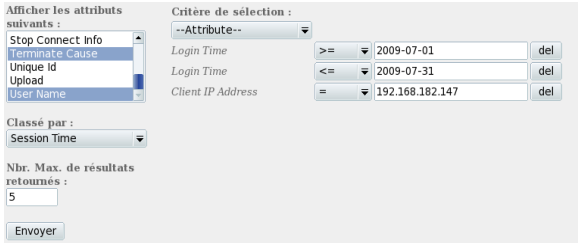


- Search Example No. 1. Display in chronological order of the connections made between June 1 and June 15, 2009 with the criteria default display:



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	[redacted]
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	

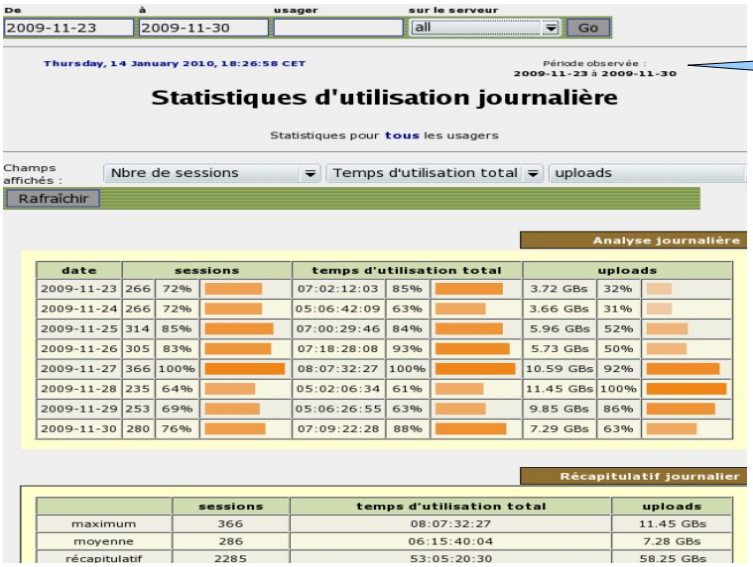
- Search Example No. 2. Showing 5 connections made during the month of July 2009 on the station whose IP address is "192.168.182.129". The display criteria includes the cause of disconnection and does not take into account the volume of data exchanged:



Client IP Address	Login Time	Logout Time	Session Time	Terminate Cause	User Name
192.168.182.147	2009-07-01 14:07:28	2009-07-01 14:08:30	1 minutes, 2 seconds	User-Request	[redacted]
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	

6.3. Daily use

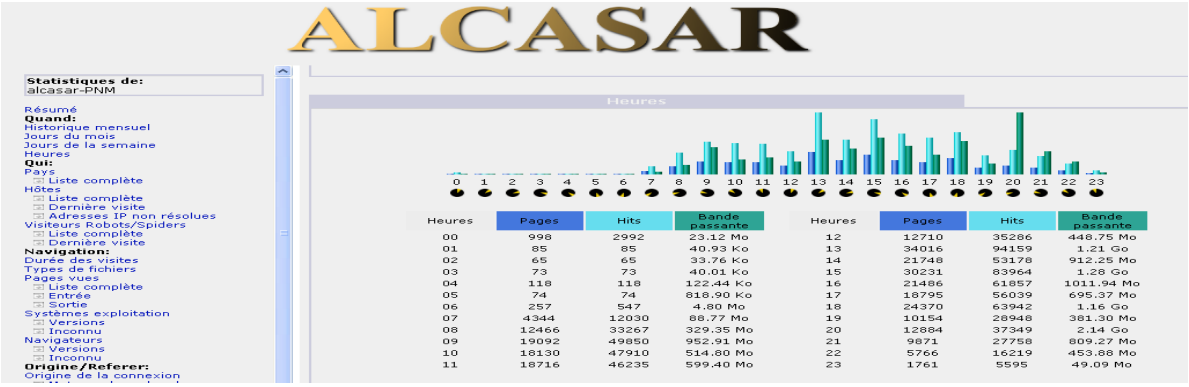
This page allows you to know the daily load of the portal.



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

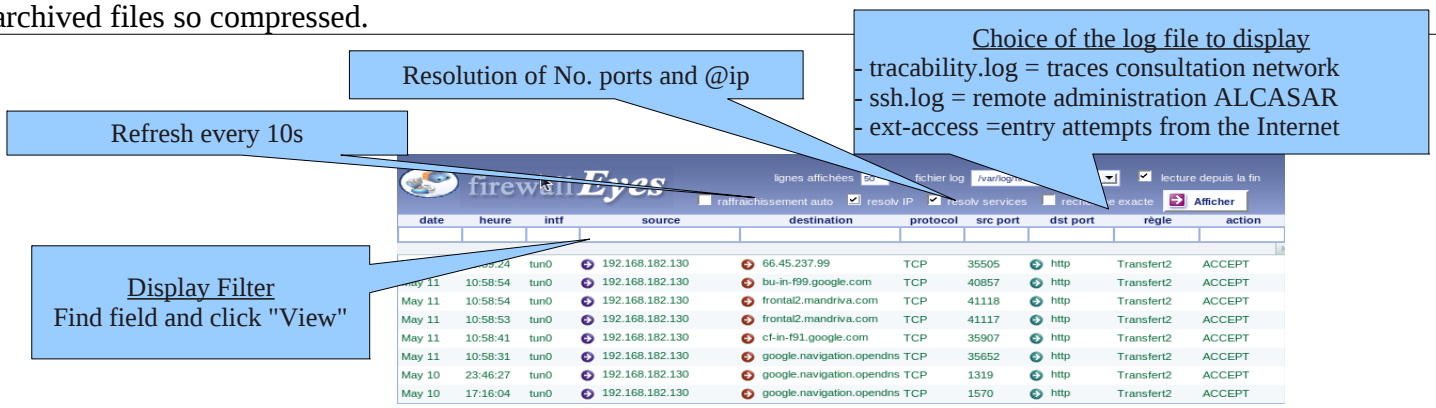
6.4. Consultation WEB

This page allows you to view the statistics of the consultation carried out by the global Web equipments on the network consultation. The statistical report is recalculated every 30 minutes from logs containing no source IP addresses or the names of users.



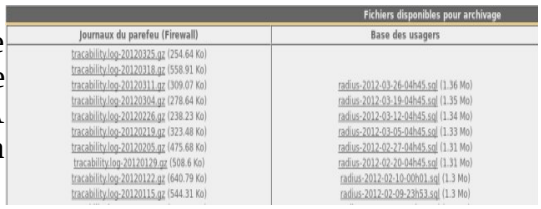
6.5. Firewall

This page allows you to view logs of ALCASAR firewall. Three families of files can be seen : traces of consultation network connection (file "tracability.log"), traces related to the administration of ALCASAR Remote (file "ssh.log") and traces of attempts entry into the network from the Internet consultation files ("ext_acces.log"). Each log file is the current week. The last few weeks are also viewable by selecting the archived files so compressed.



7. Backup connection traces

The menu "Backup" from the management interface present in the first two columns, the log files produced by ALCASAR to enable archiving ("right click" on the file name, then "save target as"). A third column contains the archives of configuration used for relocation of a gate due to a failure or a hardware change(cf. §9.4).



7.1. Logs firewall

Three families of files are available: traces of Internet connection to devices on the network consultation files (file « tracability.log »), traces related to the administration of ALCASAR Remote (file « ssh.log ») traces related to the administration of ALCASAR Remote (file « ext_acces.log »). These files are automatically generated once a week in the directory « */var/Save/logs/firewall/* » portal. Files older than one year are deleted. These files do not contain the names of users.

It is possible to generate the archive log file is currently active.

It is possible to automatically search these files. For example, whether the Internet IP address "10.10.10.10" was contacted by a station user, run the following line: : « *for i in /var/Save/logs/firewall/tracability*;do gunzip -c $i|grep 10.10.10.10; done* ».

7.2. The users database

These files (in the "SQL" format) are backups of the database users including : username, password encrypted attributes and history of opening and closing session on the portal. They are generated automatically, once a week, in the directory « */var/Save/base/* » portal. You can generate a backup at any time. Files older than one year are deleted. They can be reinjected (imported ALCASAR (§ 4.5). They are also in a relocation portal (cf. §9.4).

7.3. If Judicial Inquiry

In the context of a criminal investigation, the law enforcement officials may ask you to trace connections of your users. You just have to provide the database file users ("*radius-****.sql*") and the traces of Internet connections (" *tracability.log-***.gz* ") corresponding to the week covering the date of the offense. By correlating the information in these files, investigators can know exactly what such users, from such a position, is connected as day such a system by exploiting protocol. Investigators are asking if the corresponding files in the current week, creating an immediate backup of the user base and the log file (see previous §).

8. advanced Features

8.1. Account Management Administration

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

- « root » : This is the account of system administration ;
- « sysadmin » : This account allows you to take remote control of the system securely (cf. § next).

Alongside these two "system" accounts, "management" accounts have been defined to control functions through the center ALCASAR graphical management. These "management" accounts may belong to three profiles:

- « admin » : accounts associated with this profile can access all the functions of the management center. A first account linked to this profile was created during the portal installation (see installation doc);
- « manager »: accounts associated with this profile can only access management functions for users and groups (cf. §4) ;
- « backup » : accounts associated with this profile can only access backup and archiving log files (cf.§7).

You can create as many accounts as you want management in each profile. To manage these management accounts, use the

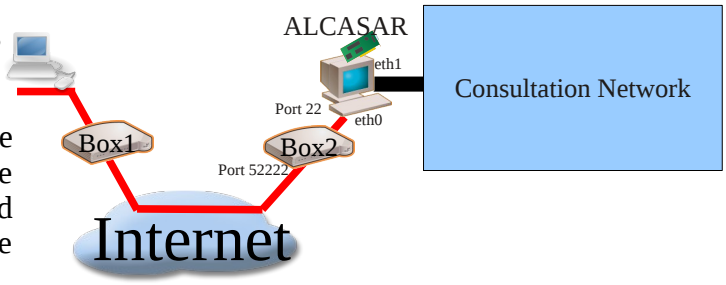
« *alcasar-profil.sh* » as « root » :

- *alcasar-profil.sh --list* : to list all the accounts of each profile
- *alcasar-profil.sh --add* : to add an account to a profile
- *alcasar-profil.sh --del* : to delete an account

- *alcasar-profil.sh --pass* : to change the password of an existing account

8.2. administration through secure Internet

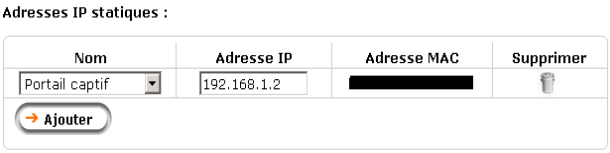
It is possible to connect to a remote ALCASAR using an encrypted stream protocol ("SSH" - Secure SHell). For example, an administrator who seeks to administer, through the Internet, a ALCASAR or equipments on the network consultation. At first, you need to activate the service "SSH" on ALCASAR (menu "system" and "network"). You must know the IP address of the Internet Box2.



a) Box Configuration

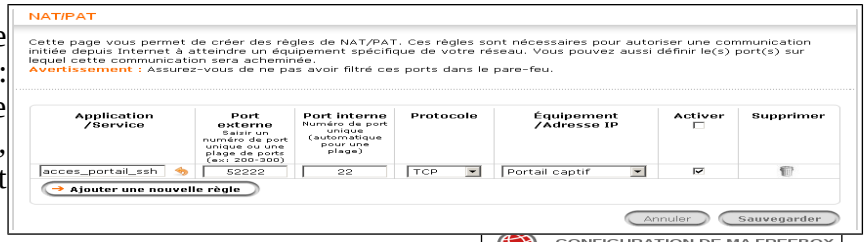
It is necessary to configure it. Lets map "SSH" protocol to ALCASAR ETH0. To "anonymize" the flow SSH on the Internet, we decided not to use the default port number (22), but another (52222). You can keep the default number or choose a new one.

- Case of a "Livebox"

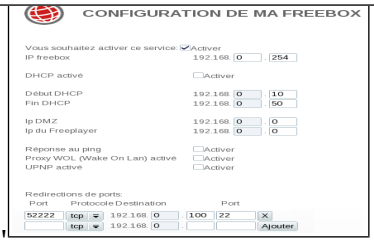


In the menu "Advanced settings", create an entry for the IP address of eth0 ALCASAR (Internet side). Same menu "Equipment Management".

In the menu "NAT / PAT," complete the following fields and save:
The external port (52222 in this case) is the port on which ssh frames arrive. Internally, ALCASAR SSH listening on its default port (22).



- Case of a « freebox »

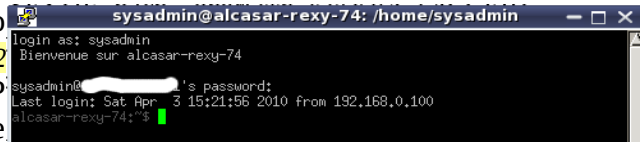


In the menu "router", configure port forwarding.

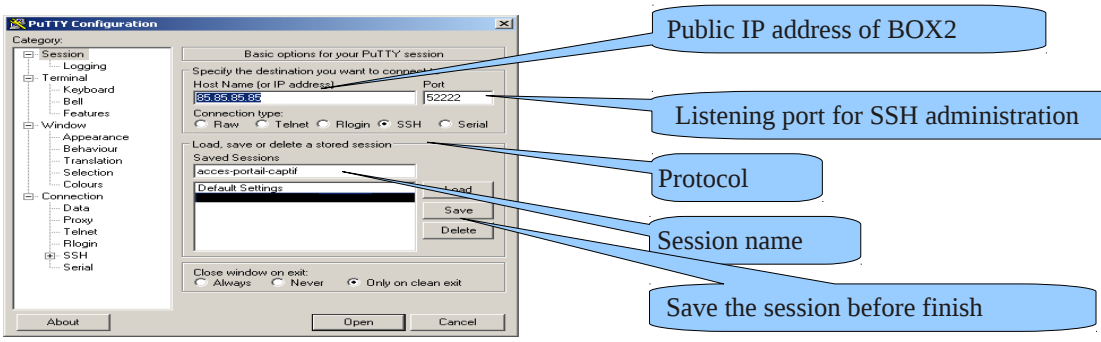
b) Administration ALCASAR text mode

You can log on to the remote operator ALCASAR the Linux account "sysadmin" created during the installation of the system. Once connected, you can use the administrative commands (see § 12.1). You can become "root" via the command "su".

- On Linux, install "openssh-client" (it is also possible to install "putty") and run the command « *ssh -p 52222 sysadmin@w.x.y.z* » (replace « w.x.y.z » by the public IP address of the BOX2 and adapt the "external_port" by the listening port number of the BOX2 (52222 in our example).



- On Windows, install "Putty" or "putty-portable" or "kitty" and create a new session:



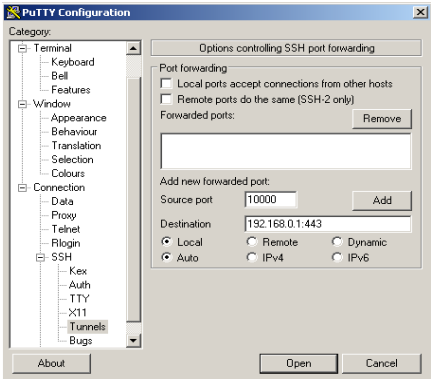
click on "Open", accept the server key and log on as "sysadmin".

c) Administration ALCASAR in graphical mode

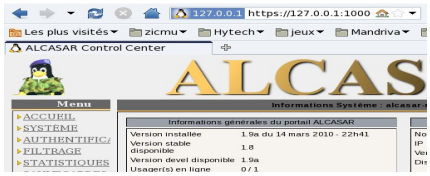
The goal now is to redirect the flow of Web browser of the management station in an SSH tunnel to ALCASAR to graphically administer. To create the tunnel:

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

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



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



d) Administration of network equipment consultation

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

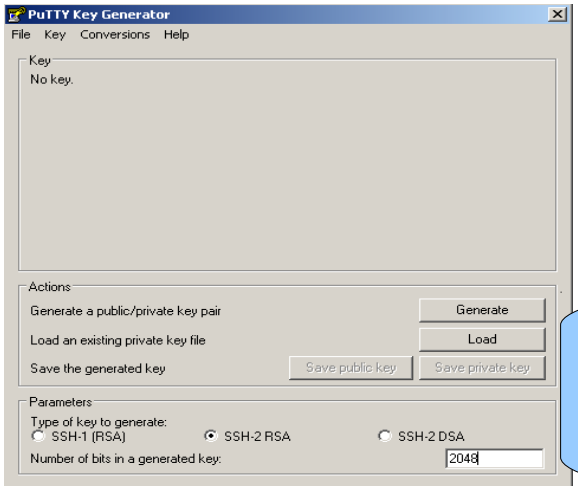
- On Linux, run the command: « *ssh -L 10000:@IP_équipement:Num_Port -p 52222 sysadmin@w.x.y.z* ».
  « @IP_équipement » is the IP address of the equipment to administer.« NUM_PORT » is the administration port of this equipment (22, 80, 443, etc.).
- On Windows, enter the IP address and port of the equipment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

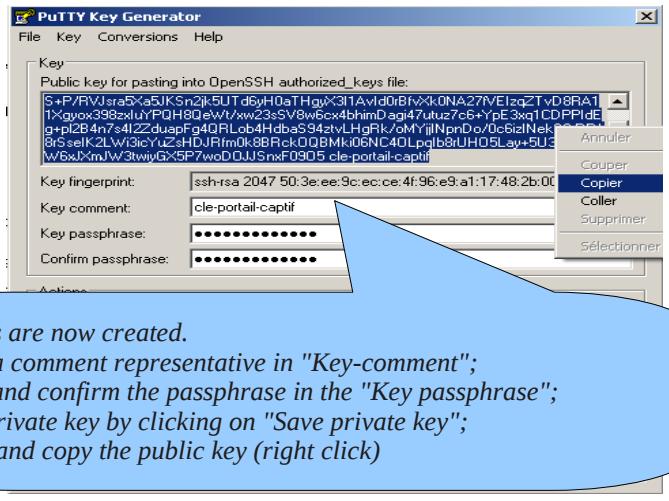
To administer via ssh, run *« ssh login@localhost:10000 »*
To use a web interface, connect your browser to the URL: *« http(s)://localhost :10000 ».*

e) Operation of SSH tunnel using a key pair (public key / private key)

This paragraph, although not essential, will increase tunnel safety administration through the authentication of the administrator's private key.

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

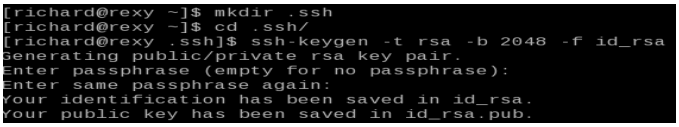




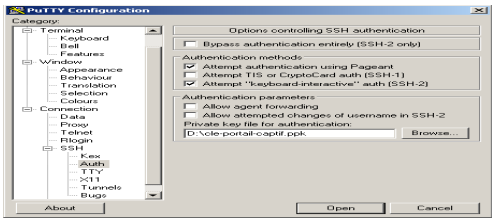
The keys are now created.
- Enter a comment representative in "Key-comment";
- Enter and confirm the passphrase in the "Key passphrase";
- Save private key by clicking on "Save private key";
- Select and copy the public key (right click)

  - Linux with« *ssh-keygen* »

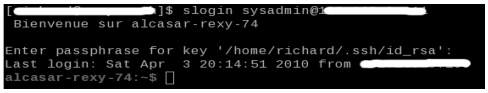
In your home directory, create the directory « *.ssh* » if there is not. From this, generate your key pair(« *ssh-keygen -t rsa -b 2048 -f id_rsa* »). Command « *cat id_rsa.pub* » can see (and copy) your public key.



- Copy the public key to the remote portal:
  - run the following command to directly copy your public key to the remote server:
    - *ssh-copy-key -i .ssh/id_rsa.pub sysadmin@<@IP_interne_consultation>*
    - Enter your password and your public key is copied to the architecture *sysadmin/.ssh/authorized_keys* automatically with the correct permissions.
  - Another method: log on via remote ALCASAR "ssh" as "sysadmin" and run the following commands: « *mkdir .ssh* » puis « *cat > .ssh/authorized_keys* » *;*
    - copy the contents of the public key from the clipboard ("Ctrl V" for Windows, middle mouse button for Linux) type« Entrée » and « Ctrl+D » ;protect the directory: « *chmod 700 .ssh* » and key file « *chmod 600 .ssh/authorized_keys* » ;check the file:« *cat .ssh/authorized_keys* », log out« *exit* ».
  - Test connection from Linux: « *slogin sysadmin@w.x.y.z* »
- Test connection from Windows:
  - load the previous session of putty;
  - on the left side, select "Connection / SSH / Auth";
  - click "browse" to select the key file;
  - select the left side Session;
  - click "Save" then "Open";
  - enter the user "sysadmin";
  - the key is recognized, it remains only to enter the passphrase.



- If you now want to deny the connection password, configure the sshd server:
  - go root (*su -*) *and set the following options file*« */etc/ssh/sshd_config* »:
    - ChallengeResponseAuthentication no
    - PasswordAuthentication no
    - UsePAM no
  - restart the sshd server(« *service sshd restart* ») and close the ssh session(« *exit* »).



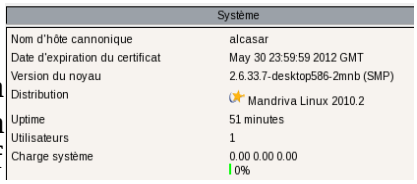
8.3. Implementation of the organization's logo

It is possible to put in place the logo of your organization by clicking on the logo at the top right corner of the management interface. Your logo will be inserted in the authentication page and in the top bar of the management interface. Your logo should be free format "png" and must not exceed the size of 100KB. It is necessary to refresh the browser page to see the result.

8.4. Manipulation with the server certificate

ALCASAR crypt exchanges with equipments on the network consultation in the following cases:

- for users: authentication request and changing passwords;
- for administrators: access to graphical control center (ACC).



Encryption uses TLS associated with a server certificate and a certification authority local (AC) created during the installation. This server certificate with a lifetime limited to 4 years, you can see the expiration date in the front page of the Control Center Graphics:

Upon expiration of the certificate, you can regenerate via the command« alcasar-CA.sh ».

It will be necessary to remove the old certificate store browsers before importing / accept the new.

a) Installation of an official certificate

Since version 2.0 it is possible to install an official certificate type "intranet" offered by some suppliers. The integration of such a certificate prevents windows security alert on browsers that have not integrated the root certificate of ALCASAR (cf. §2.2.b). Unlike certificates "Internet" certify a registered domain name with a registrar, a certificate "intranet", may certify a private IP address or a simple name server (hostname). This corresponds to the situation ALCASAR including the "hostname" is always "ALCASAR." To gain your certificate, follow the instructions on the provider's site knowing that the web server is operated by a server ALCASAR "APACHE" with SSL module. The following example allows the integration of a certificate "intranet" generated by the supplier "Digitalix." At first, you need to run the following command on ALCASAR as "root" : *openssl req -newkey rsa:2048 -new -nodes -keyout alcasar.key -out alcasar.csr* This command generates two files : the private key (*alcasar.key*) and the certificate request (*alcasar.csr*). Copy the certificate request file on a USB key in order to copy its contents to the vendor's site. It must return a file containing your server certificate Official (*alcasar.crt*). If applicable, you must also get the intermediate CA certificate from your provider (for Digitalix, it is available here: http://www.digitalix.fr/certs/HACert-bundle.crt).
As "root", copy the three files « *alcasar.key* », *alcasar.crt* » and « *HACert-bundle.crt* » in your home directory (*/root*). Then perform the following operations:

1. *cd /etc/pki/tls* (moving certificate in the directory)
2. *mv certs/alcasar.crt certs/alcasar.crt.old* then *mv certs/server-chain.crt certs/server-chain.crt.old* and finally *mv private/alcasar.key private/alcasar.key.old* (backup the old certificates)
3. *cp /root/alcasar.crt certs/* et *cp /root/alcasar.key private/* (copy of the official certificate and its private key)
4. if your provider has a intermediate CA certificate: *cp /root/HACert-bundle.crt certs/server-chain.crt else* : *cp certs/alcasar.crt certs/server-chain.crt*
5. Restart the Apache Web server via the command« *service httpd restart* ».

In case of problems:

- go back by reversing the operations of the second line, or you can recreate the local certificates "brand new" via the command« alcasar-CA.sh » ;
- restart the Apache Web server via the command« *service httpd restart* ».

b) Copy of certificate on multiple ALCASAR

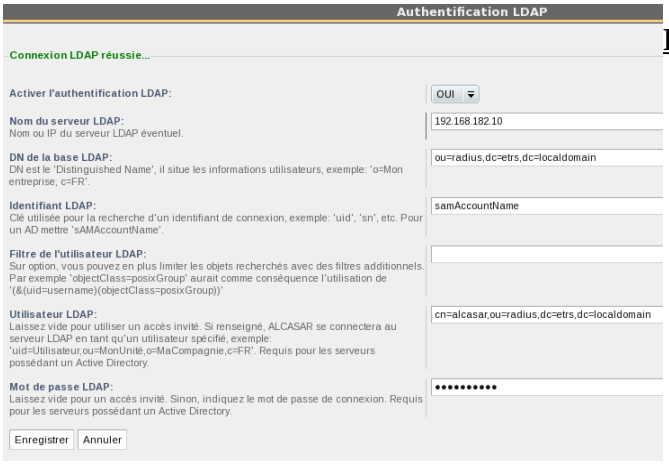
If you operate several ALCASAR, it may be useful to copy the certificate from a reference ALCASAR others. If you have installed an official certificate, perform steps 1 through 5 of the previous chapter on the various ALCASAR. In the case of a certificate created during installation, copy the following files from the five reference ALCASAR others:

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

Restart the Apache Web server via the command: « *service httpd restart* ».

8.5. Using an external directory server (LDAP or AD)

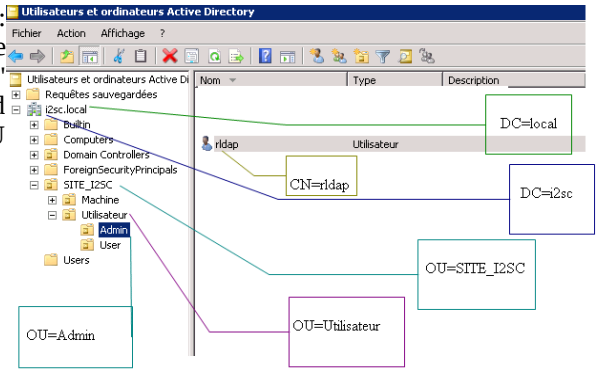
ALCASAR integrates a module allowing to query a external directory server (LDAP or AD) located either LAN or WAN side. When this module is enabled, ALCASAR primarily uses the external directory, then in case of failure, the local database to authenticate a user. In all cases, the log files related to user events (log) are treated in the local database of ALCASAR. The management GUI of this module is as follows:



Remark :

- attributes of users located in the external directory can not be changed via the management interface of ALCASAR;
- use secure protocol "ldaps" is not available at this time. The network segment between ALCASAR directory and must be controlled, for obvious safety reasons (cf. § 10);
- External directories do not support case sensitive unlike the local database of ALCASAR.

Example: This screenshot shows the AD directory tree organized as follows: standard users are placed in the Organizational Unit (O.U.) "User". The account used by ALCASAR to see the remote directory is the account "rldap" located in the OU "Admin". This account is a standard that does not need special rights. Both O.U. "Admin" and "User" are located themselves in OU "User".



- DN de la base : « ou=User,ou=Utilisateur,ou=SITE_I2SC,dc=i2sc,dc=local »
- Identifiant LDAP : « sAMAccountName »
- Filter: vide
- User LDAP : « cn=rldap,ou=Admin,ou=Utilisateur,ou=SITE_ISC,dc=i2sc,dc=local »
- Password : password of the user « rldap »

It is possible to assign all users declared in an external directory (LDAP or AD) ALCASAR specific attributes (bandwidth, concurrent session, etc.).. To do this, declare a group named "ldap" for which you set the desired attributes. It is also possible to assign attributes to a particular account ALCASAR authenticated on an external directory. To do this, create a user with the same name ALCASAR that directory.

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

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

a) Windows DNS Management

When an AD architecture is present on the network and consultation stations are hung up on Windows domain controller, they must apply to both the controller for DNS resolutions specific to Windows services and DNS of ALCASAR for Internet access. One solution is to configure the DNS ALCASAR so it redirects the DNS domain controller queries concerning. In this way, the equipment consultation are configured as single ALCASAR DNS.

The only change to make is to add the following line in the file « */etc/sysconfig/dnsmasq* » :

OPTIONS= " --server=/<your.domain>/<@IP_SRV-AD-DNS> "
Example : *brock.net* domain is managed by a server AD / DNS with the IP address 192.168.182.10 is. The line to add is: *OPTIONS=" --server=/brock.net/192.168.182.10 "*
Please note that it is the domain name and not the server srv-ad.brock.net.
Dnsmasq restart the service for your changes to be applied(« *service dnsmasq restart* »).
Reminder: the DNS suffix 'localdomain' stations in fixed address must be present.

b) Using an External DHCP Server

Using an External DHCP Server «*/usr/local/etc/alcasar.conf* ») :

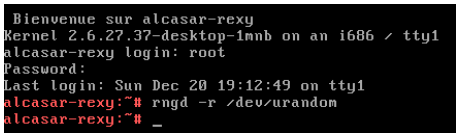
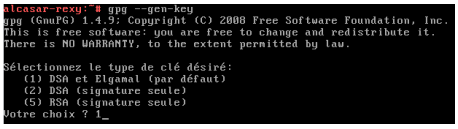
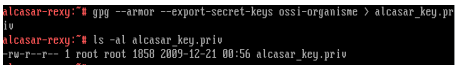
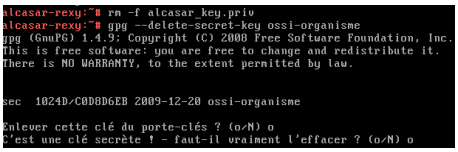
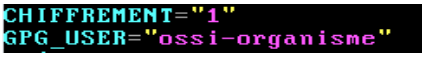
- EXT_DHCP_IP=<@IP_srv_externe>
- RELAY_DHCP_IP=<@IP_interne_ALCASAR>
- RELAY_DHCP_PORT=<relay port to the external DHCP server> : (default 67)

The external DHCP server must be configured to provide stations:

- a range of IP @ corresponding to the range allowed by ALCASAR (default 192.168.182.2-254/24);
- gateway address corresponding to the internal IP address of ALCASAR (default 192.168.182.1); DNS suffix "localdomain";
- the @ DNS server IP -> IP address internal ALCASAR (default 192.168.182.1);
- the @ IP of the time server (NTP) -> the internal IP address of ALCASAR (default 192.168.182.1) or the domain controller (to avoid temporal drifts, also to ensure the implementation position automatic time therefor to a server matched to the Internet or more simply ALCASAR).

8.7. Encryption of log files

ALCASAR can automatically encrypt log files of firewall, http proxy “squid” and access to the management interface. For this, it uses the asymmetric algorithm (GPG public key + private key). Providing the private key to a responsible body for your receiver, you protect administrators ALCASAR charges change these log files. In case of inquiry, simply provide log files and encrypted private key for decryption. The procedure for activating the encryption is as follows:

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

Infos :

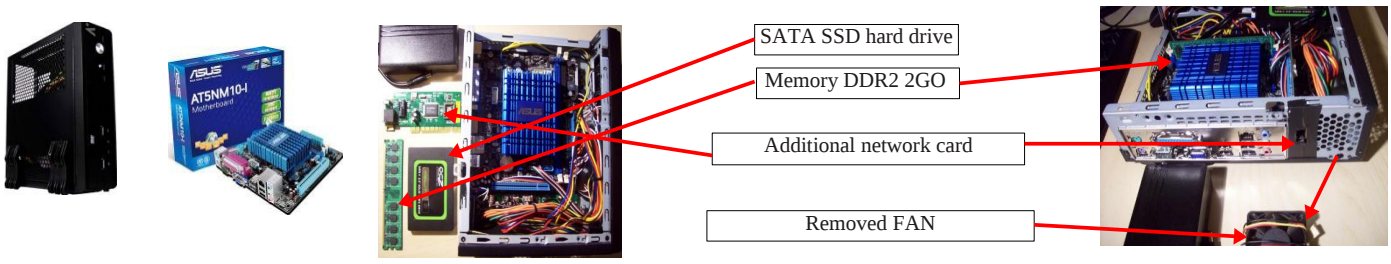
- ALCASAR uses the keyring "root" in the directory « */root/.gnupg* » ;
- '*gpg –list-key*' : allows to list all the key pairs contained in this kit;
- '*gpg --delete-key* <*user_name*>*' :* deletes a public key keyring;
- '*gpg --delete-secret-key* <*user_name*>' : deletes a private key keyring;
- You 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* <*filename_crypt_archive*>'.

8.8. Load balancing connection

ALCASAR has a script to distribute connections to several gateways to the Internet.
To date, the parameters are not included in the management interface, it is necessary to modify the script: "*alcasar-load-balancing.sh*" located in "/usr/local/sbin".
Virtual network cards Internet side must be mounted first.
Note that in this version, it does not test connectivity to the Internet. Delays may occur if the gateway is no longer operational.

8.9. Create a dedicated housing ALCASAR

This chapter presents an embodiment of a dedicated housing (appliance) ALCASAR economic constraints which are miniature (mini-itx) without noise (noiseless), fan (fanless) and low energy consumption. The configuration is as follows: Case A + Case CS160 (12V integrated) motherboard AT5NM-10 (integrated Intel D525), 2GB of DDR2 memory (PC2-6400) HDD 2.5 '200GB SATA, PCI Ethernet complementary. Replacing the hard drive with a SSD 2.5 "40GB reduces the heat, remove the blower housing and thus reduce the consumption of 28W to 20W. The cost of this configuration is around 210 € (shipping included). The cost is the annual electricity consumption of 20.53 € (20 * 24 * 365/1000 * 0.1152). ALCASAR is installed via a USB drive as usual. Once deployed, the unit requires no keyboard, no mouse or screen.



8.10. Bypass the portal

For reasons of maintenance or emergency, a workaround portal was created. It eliminates user authentication and filtering. Logging network activity remains active. Accountability connections is no longer assured.
To start bypassing the portal, run the script « *alcasar-bypass.sh --on* ». To remove it, run the script « *alcasar-bypass.sh --off* ».

9. Stop updates and resettlement

9.1. Shutdown

Two possibilities can stop properly the ALCASAR PC :

- by briefly pressing the power button of the equipment;
- by connecting to the console as root and running the command "init 0";

When restarting the PC ALCASAR a procedure deletes all connections that have not been closed due to a stop unwanted (failure, power failure, etc.).

9.2. Updates of the operating system

Mageia-Linux provides an excellent mechanism to implement such security fixes (patches) on the system and its components. ALCASAR has been developed to be fully compatible with this mechanism. So, every night at 3:30, the security updates are retrieved authenticated and applied where appropriate. You are of course possible to manually initiate the update by the command « *urpmi –auto --auto-update* » as « root ».
Once the update is complete, a message may warn you that a system reboot is required. This message appears only if a new kernel (kernel) or a major library were updated.

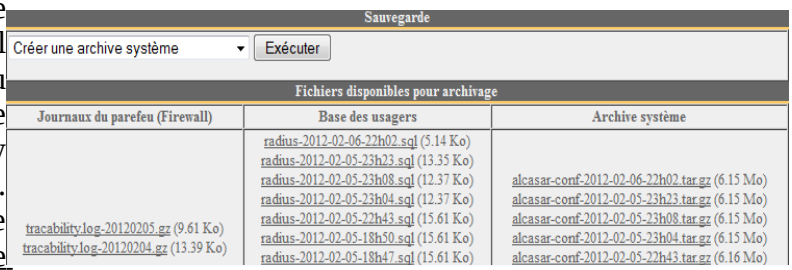
9.3. Update ALCASAR

You can tell if an update is available for ALCASAR looking cover page of your management interface or by running the command « *alcasar-version.sh* ». Retrieve and untar the latest version as in a normal installation. Run the installation script (« *sh alcasar.sh --install* »), it will automatically detect the previous version and ask if you want to perform an update. During an update, the following data are given:

- network configuration;
- the name and logo of the organization;
- usernames and passwords for administrative accounts of the portal;
- based users and groups;
- blacklists primary and secondary;
- the list of sites and MAC addresses of trust;
- configuration of network filtering
- certificates of the Certification Authority (CA) and the server.

9.4. Replacing a portal

ALCASAR incorporates a device to reinstall portal with its parameters. This can be useful when changing the PC support following a change or a hardware failure. Start generating an archive portal configuration via the management interface (menu "backup" + "create an archive system"). Retrieve the generated file on a USB key. Install the new operating system as in an initial installation. Connect your USB and copy the file "archive system" in the directory « */tmp* » under the name « *alcasar-conf.tar.gz* ». Retrieve and untar the latest version and install the ALCASAR as in a normal installation: « *sh alcasar.sh --install* ».



10. Diagnostics

This chapter presents various diagnostic procedures in different situations or questions encountered. Orders (*emphasis* in yellow) are engaged in a console as "root".

10.1. Network connectivity

- test the status of network cards: : run the commands « *ethtool eth0* » and « *ethtool eth1* » to verify the status of the two network cards (« *Link detected » and « Speed* » fields example) ;
- test connection to the output router : start a « *ping* » to the router's @IP Output (Box F.A.I). In case of failure, check the network cable, the interface configuration eth0 (*ifconfig eth0*) and router status;
- test connection to external DNS servers : start a « *ping* » to the DNS server's @IP . In case of failure, change servers;
- test the internal DNS server(dnsmasq) : initiate a request for name resolution (ex. : *dig www.google.fr*). In case of failure, check the configuration file "dnsmasq" (*cat /etc/dnsmasq.conf*).
  To verify the proper functioning of the service or redirections (in the case of an internal DNS server), you can uncomment the first line of the file OPTIONS */etc/sysconfig/dnsmasq* to view requests and responses (*tailf /var/log/dnsmasq/queries.log*). Warning : this is relatively resource intensive. It is preferable once validated, this option is commented on again. To be taken into account, these changes always require restarting the service dnsmasq : « *service dnsmasq restart* » ;
- test Internet connectivity: run the command « *wget www.google.fr* ».If successful the front page of Google is downloaded and stored locally (index.html). The menu "system / service" management interface reports this test;

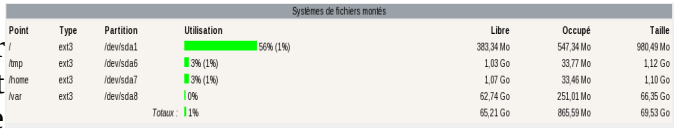
- connectivity test equipment to consultation : you can test for the presence of a device on the network via the command consultation « *arping -I eth1 @ip_quipment* ».

You can view all devices on the network by running the consultation« *arpscan eth1* » ;

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

You can view the network packets from the network consulting installing tool « tcpdump » (urpmi tcpdump) and running the command « tcpdump -i eth1 ».

10.2. Available disk space



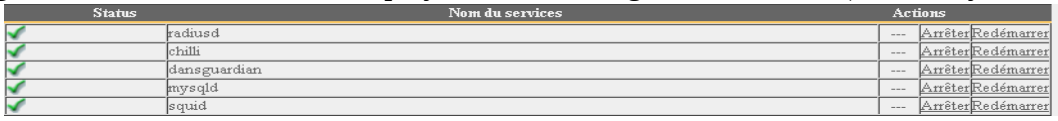
If disk space is not enough, some modules may no longer work. For example, the proxy server "Squid" stops when it can no longer feed its log files. You can check the available disk space (especially partition */var*) :

- in graphical mode via the homepage of the management center;
- 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/**).

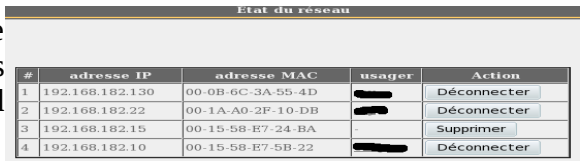
10.3. Services server ALCASAR

To fulfill these tasks, ALCASAR operates several services server. Stopping one of them can prevent ALCASAR run. It is useful to know how to diagnose why a service is stopped. Run the command « *ps fax* » and verify that the web server apache '("httpd") is running. If necessary, start with the command « *service httpd start* ». In case of failure, view the log report error via the command « *tailf /var/log/httpd/error.log* ».
The operating status of other services is displayed in the management interface(menu « system/services ») :



You can stop or restart via the management interface or via the command "service service_name start / stop / restart". In case of failure, check the system log file (*tailf /var/log/messages*) why they can not get started.

10.4. Connectivity equipment consultation



On the management interface (under "System / Activity"), make sure that your equipment consultation have correct network settings (MAC address / IP address). If this is not the case, delete the old address by registered ALCASAR and reconfigure equipment.
Consultation on equipment :

- check the network settings: run « *ipconfig /all* » on Windows, « */sbin/ifconfig* » on Linux ;
- if they are not correct, change them. For equipment in dynamic mode, restart an address request : « *ipconfig /renew* » on Windows, « *dhclient eth0* » on Linux.

If the interface is not configured, check the cables and make sure that the DHCP frame pass over the network (using the frame analyzer "wireshark" for example). On ALCASAR console, you can see the incoming requests by running the command « *tailf /var/log/messages* » or displaying the terminal N°12 (<Alt> + F12).

```
Dec 29 22:31:27 alcasar      coova-chilli[2299]: chilli.c: 2694: New DHCP reques
t from MAC=08-00-27-E7-EA-89
Dec 29 22:31:27 alcasar      coova-chilli[2299]: chilli.c: 2661: Client MAC=08-0
0-27-E7-EA-89 assigned IP 192.168.182.129
```

- Test connection to the portal : start a ping to the IP address of ALCASAR. In case of failure, check cable and configure the network interface.
- Test name resolution : On Windows, run « *nslookup alcasar* ». On Linux, run « *dig alcasar* ». The result should be the IP @ ALCASAR. In case of failure, check qu'ALCASAR is indeed the DNS server equipment consultation
- Management Interface : Open a browser on equipment consultation and try to log on ALCASAR (http://alcasar).
- Test Internet Connection : Test the connection to a website. ALCASAR must intercept you and submit the authentication window.

10.5. Connection to ALCASAR with a serial terminal

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

File */etc/inittab* :

- save the original : *cp /etc/inittab /etc/inittab.save*
- edit the file : *vi /etc/inittab*
  before this line : « # Single user mode », add the following lines:
  #connexion au terminal serial
  s0:2345:respawn:/sbin/agetty -L 9600 ttyS0 vt100 -f /etc/issue
  then save « Esc »then « :wq! »

File */etc/securetty* :

- save the original : *cp /etc/securetty /etc/securetty.save*
- edit the file : *vi /etc/securetty*
  add one of the two following line at the end of file:
  ttyS0 *if using a 9-pin serial port*
  ttyUSB0 if using a Serial / USB
  and save «Echap» and « :wq! »
- run the command« *init q* » to account for this change.

To see the output of the boot in GRUB, edit the file */boot/grub/menu.lst*

- save the original: *cp /boot/grub/menu.lst /boot/grub/menu.lst.save*
- in the section 'title linux' after adding vga=791 to end of line :
  console=tty0 console=ttyS0,9600n8 by standard serial port
  console=tty0 console=ttyUSB0,9600n8 in USB port

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

10.6. Problems experienced

This chapter presents the feedback from organizations who have found the solution to the problems identified.

a) The images do not appear on some sites

When filtering domains and URLs is enabled, the default filter ALCASAR web links without domain name (IP address to pure). Thus, the web pages containing this type of link are shown only partially. Two solutions to avoid this behavior: remove the "IP" blacklist (cf. § 4.1.b) or register the IP addresses contained in these web links as "rehabilitated site" (cf. § 4.1.c). For example, the website "leboncoin.fr" link all images to the following IP addresses: 193.164.196.30, .40, .50 and .60 and 193.164.197.30, .40 and .50.

b) Navigation impossible with some antivirus

Disable the "web-proxy" integrated some antivirus (if trend-micro). This function uses a white/black list which is recoverable on live servers TrendMicro (backup30.trendmicro.com, etc..) And analysis/validates every request for a site... It is activated by a user rights limited, to avoid disadvantage to this feature incompatible with proxies of ALCASAR, it is best to stop the service "Trend Proxy Service" and restart the station.

c) Windows Stations previously connected to a public hotspot

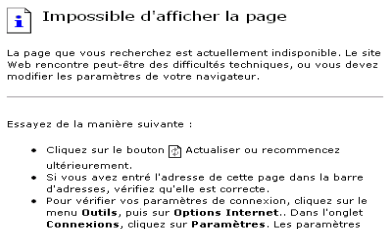
When a system connects to a "public hotspot", it provides network parameters and a "lease" which determines the validity time of these parameters. Windows XP stations do not reset these settings during a reboot. Thus, even if they change network, they will come with Hotspot previous settings. This problem is recognized by Microsoft that offers the following solution: force 'by hand' renewal application network settings via the command: « *ipconfig /renew* ».

d) Stations Windows fixed address

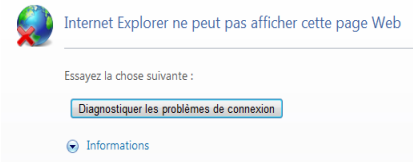
It is necessary to add the DNS suffix "localdomain" (network configuration + “advanced” + “heading dns ").

e) Can not navigate while you access the portal page (http://alcasar)

This can occur after a complete reinstallation of the portal or after an update with change server certificate. Browsers have then the following pages when they attempt to join a website:



With IE6



With IE 7 - 8 and 9

With Mozilla

This is due to the fact that browsers try to authenticate the portal ALCASAR using an old certificate. On browsers, we must remove the old certificate ALCASAR ("tools" + "Internet Options", tab "content" button "Certificates" tab "root certification authorities") to replace the latter as described in § 2.3.1.

f) Can not navigate after completing the "trusted sites"

ALCASAR verifies the validity of domain names entered in this section (cf. § 3.7.a). If a domain name is not valid, the service 'chilli' can no longer start. Then change the domain name with a problem and restart the service 'chilli' via the command « *service chilli restart* ».

g) Overload memory and system

The Linux system always tries to exploit the maximum RAM. On the home page management center, the bargraph indicating the use of physical memory can regularly be found beyond 80% and appear red. This is normal.
If the system needs more memory, it will use the swap. This swap is an area of the hard disk operates as RAM (but 1000 times slower). If you find that the system uses swap space (> 1%), you can consider increasing the RAM to significantly improve system responsiveness especially when the filter module and domain URL is activated .
You can view the system load on the home page of the management center in the 'System / load system, or console using the command « *top* » ou « *uptime* » :

- 3 values shown represent the system load average for the last 5 and last 15 minutes. The load average is the number of processes waiting for CPU usage.
  These values are normally less than 1. A value greater than '1 .00' results under-sizing of the server (especially if it affects the three values (payload included in the length).
- Search process that monopolizes a large percentage of the load (command « *top* »).

11. Secure

On consultation network, ALCASAR is the way to control Internet access. It also helps protect the network vis-à-vis the outside or vis-à-vis a pirate house. To this end, it includes:

- protection against theft of identifiers. The authentication flow between devices and users ALCASAR are encrypted. Passwords are stored encrypted in the database;
- protection against disconnection omissions. The attribute "time limit of one session" (cf. § 3.1) allows a user to disconnect automatically after a set time;
- protection against outages (network or equipment consultation). Users whose equipment does not respond consultation for 6 minutes are automatically disconnected;
- protection against session hijacking spoofing network settings. This spoofing technique exploits the weaknesses of protocols "Ethernet" and WIFI. To reduce this risk, ALCASAR tamper incorporates a process is running every 3 minutes (*alcasar-watchdog.sh*) ;
- protection bootloader portal (GRUB) password. This password is stored in the file « */root/ALCASAR-passwords.txt* ».

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

11.1. On ALCASAR

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

11.2. The consultation network

a) Network type "hotspot"

These networks are "open" in nature and they often exploit WIFI technology:

- on WiFi access points (AP) Enable WPA2 encryption "personal." This avoids listening WIFI traffic by a user (even if the key is the same for everyone). You can choose a simple WPA2 key as your organization name for example;
- on Ethernet switches, enable "DHCP snooping" on port operated by ALCASAR well as the interswitch ports. This will prevent false DHCP servers (Fake DHCP servers).

b) Controlled networks

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

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

Equipment consultation can (should) incorporate several security features such as locking the BIOS setup and office, antivirus, automatic update security patches (patch), etc.. To facilitate downloading security patches or updated antivirus (cf. § 7), ALCASAR may authorize equipment to automatically connect without authentication on sites specifically identified.
If you want to set up stations consultation free access, it may be worth your press products ensuring both the protection of the privacy and security consultation station (station type "cafe") . These products allow the user to partition in a sealed environment. At the end of a session, the user environment is clean.

- Stations for Linux, you can install the product "xguest" (it is provided natively in the case of Mandriva, Fedora and RedHat)
- For stations on Windows, follow this link to the Microsoft TechNet ©:
  « http://technet.microsoft.com/fr-fr/library/gg176676%28WS.10%29.aspx »

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

12. Annexes

12.1. Useful commands and files

The administration of ALCASAR is used directly in a terminal command line (as 'root'). These commands all start with "alcasar-... ". All these commands (shell scripts) are located in the directories « */usr/local/bin/* » and « */usr/local/sbin/* ». Some of them rely on the central configuration file ALCASAR (« */usr/local/etc/alcasar.conf* »). With the argument "-h", each command lists the options it has.

- alcasar-bl.sh {-on/-off} : enables / disables the filtering domains and URL;
  - {-download} : download and apply the latest version of the BlackList Toulouse;
- alcasar-bypass.sh {-on/-off} : active mode on / off « BYPASS » ;
- alcasar-CA.sh :creates a local CA and server certificate. Requires restarting the Apache web server (*service httpd restart*) ;
- alcasar-conf {-apply} : apply the network settings according to the configuration file;
- alcasar-dg-pureip.sh {-on/-off} : enables / disables the filtering of URLs containing IP addresses (instead of a domain name);
- alcasar-havp.sh {-on/-off} : enables / disables the antivirus filtering flows WEB;
  - {-update} : am updating the knowledge base of antivirus(clamav) ;
- alcasar-https.sh {-on|-off} : enables / disables the encryption authentication flow;
- alcasar-load-balancing.sh : script for aggregating several distinct internet access. To run this script must be set in order to take into account the location, number and weight of the bridge (box) available.
  This script is not running automatically at server startup, once validated, can be added in the file */etc/rc.local* under the line « *touch /var/lock/subsys/local* ». To verify proper operation, run the command: *ip route*.
- alcasar-logout.sh {username} : disconnect users <username> all its sessions;
  - {all} : disconnects all connected users;
- alcasar-mysql.sh {-import fichier_sql.sql} :imports a user base overwrites the existing
  - {-raz} : reset the user base;
  - {-dump} : create an archive of the current user base in« /var/Save/base » ;
  - {-acct_stop} : stopsessions open accounts;
- alcasar-nf.sh {-on/-off} :enables / disables the filtering of network protocols;
- alcasar-rpm-download.sh : compares the version ALCASAR active with the latest version available on the Internet;.
- alcasar-safesearch.sh {-on/-off} : active/désactive le filtrage « mineur » major search engines;
- alcasar-version.sh : compares the version ALCASAR active with the latest version available on the Internet;

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

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

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

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

Sauvegarder un fichier - quitter vi

:w	sauvegarde le fichier (penser à *w*rite)
:wq	sauvegarde le fichier et quitte vi (*w*rite and *q*uit) équivallent à :x
:q	quitte vi sans sauvegarder les modifications (*q*uit)
:q!	quitte immédiatement, sans rien faire d'autre
:w <*nom_de_fichier*>	sauvegarde le fichier sous le nom <*nom_de_fichier*>
:w	*sauvegarde le fichier (penser à write)*
:wq	sauvegarde le fichier et quitte vi (*w*rite and *q*uit) équivallent à :x
:q	quitte vi sans sauvegarder les modifications (*q*uit)
:q!	quitte immédiatement, sans rien faire d'autre
:w <*nom_de_fichier*>	sauvegarde le fichier sous le nom <*nom_de_fichier*>

Copier-Coller

Y	copie une ligne, donc la place dans un tampon, pour pouvoir ensuite la coller (*y*ank, tirer)
*n*Y	copie *n* lignes
p	colle les lignes après le curseur (*p*aste, coller)

Annuler ou répéter des modifications

u	annule la dernière modification (*u*ndo, défaire)
.	(un point) répète les dernières modifications

Insérer du texte

i	active le mode insertion

Supprimer du texte

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

Rechercher et remplacer

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

12.2. Exceptions authentication helpful

The following values allow network devices to access consultation:

- to the activation of licenses,
- testing connectivity of the Internet,
- updated Microsoft system,
- update and TrendMicro antivirus clamav,
- test client version mozilla and modules,
- ...

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

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

Domains are also configurable via the management interface or directly in the file:
"*/usr/local/etc/alcasar-uamdomain*":

```
uamdomain=".download.microsoft.com"
uamdomain=".download.windowsupdate.com"
uamdomain=".ds.download.windowsupdate.com"
uamdomain=".microsoft.com"
uamdomain=".update.microsoft.com"
uamdomain=".update.microsoft.com.nsatc.net"
uamdomain=".windowsupdate.com"
uamdomain=".windowsupdate.microsoft.com"
uamdomain=".trendmicro.com"
uamdomain=".activeupdate.trendmicro.com"
uamdomain=".akamaiedge.net"
uamdomain=".akamaitechnologies.com"
uamdomain=".clamav.net"
```

It is necessary to restart the service chilli if files are changed directly.

12.3. Sheet of User

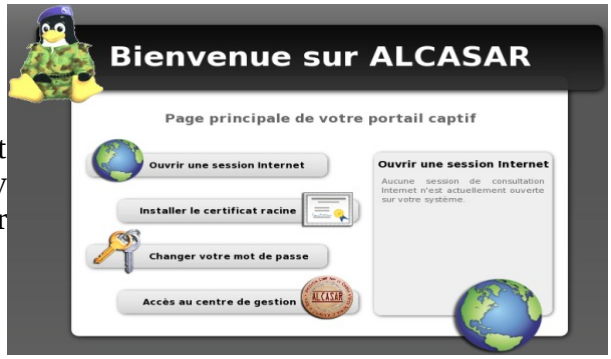
Internet access control has been implemented in your organization through a portal ALCASAR. When your browser tries to connect to the Internet, the following login window identifies you. Case is taken into account ("smith" and "Smith" are two different users).

When authentication is successful, the window "pop-up" is presented next. It allows you to disconnect from the portal (closed session). This window provides information on the rights granted to your account (expirations, download limits, list of recent connections, etc.)..

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

If connection fails, a message can know the cause: Account expired, download volume reaches maximum, attempting to connect to the outside slots allowed, etc..

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



The portal has a anmalware protecting flows WEB. It incorporates a filtering device sites whose content may be objectionable. It also helps to know when the Internet connection does not work (equipment failure or operator failed link). The following pages are displayed: