TURN YOUR WI-FI UP

UCOPIA White Paper

June 2017

Table of contents

Table of figures

1 Introduction

According to IDC (http://www.idc.com), there are 75 million mobile workers in Western Europe. Mobile workers spend up to 70% of their working time outside their office. In fact, the number of workers without a desktop has reached 46 million last year with an augmentation of 4.4% per year (Gartner). Mobile workers need to connect from meeting rooms, branch offices, or hotel rooms. Wherever pervasive network connectivity is available, employees connect an additional 1h45 minutes each working day, leading to a 22% productivity improvement (Source NOP World). In other words, mobility generates more flexibility, more usage and more efficiency. Forester Research has published a study showing that 38% of companies are providing a network access to at least 20 visitors. The same study has also highlighted that 11% of these companies had more than 200 visitors connected per month.

Companies already have wired IP backbones allowing conveying voice and data, and are continuously expending and integrating Wi-Fi wireless technologies. Deployment of pervasive networks consist of merging their infrastructure to answer the needs of multiple population of users (employees, clients, providers) and multiple uses (Internet Access, business applications).

Moreover, the rise of mobile devices transforms usages, 60% of the Internet traffic comes from mobile devices (Comscore). In 2020, Wi-Fi will handle more than 80% of mobile traffic (Cisco).

In this context, security becomes an essential concern: users and terminals authentication, access control depending on the user ID, profile but also the location and date of connection, tracking of connections and network usage must be kept to follow legal guidance. Simplicity of use and users management (account creation, access right management, technical support, etc.) defines the efficiency of pervasive network and return of investment of companies.

Beyond security, organizations want to transform their Wi-Fi investment into a revenue opportunity (value-added services, advertising revenue, etc.). According to Gartner, the Wi-Fi market will grow to $ 3.7B in 2011 to $ 9.7B in 2017 representing an annual growth of 57% for operators and 17% for enterprises.

With UCOPIA, employees, clients, partners and visitors can connect into their professional environments; simply get access to shared network resources (such an Intranet, Extranet or Internet) and still have the guaranty of advance security and quality of service. UCOPIA also brings an answer to organizations that want a return on investment of their Wi-Fi infrastructure thanks to its Analytics and marketing campaigns services.

UCOPIA develops and sells two lines of products: UCOPIA Advance and UCOPIA Express. UCOPIA Advance is designed to be installed on specific projects (many users, multiple sites, integration with a complex network) of enterprises, campus, administrations, exhibition centers and stadium. UCOPIA Express targets small projects (one site, few dozen of simultaneous connections) but is focused on simplicity of integration and exploitation. UCOPIA Express has multiple references in primary schools, secondary schools, hotels, hospitals and small and medium businesses.

This white paper describes the UCOPIA solution as a whole, all lines of product taken together. This white paper is organized as follow: A presentation of the different components of the UCOPIA solution and their main functionalities A detailed description of the architecture of the UCOPIA solution and the role of each of its components and modules The integration of the UCOPIA solution on existing network architectures multi-sites and mono-site network architectures using UCOPIA. High Availability architecture including redundancy and load-balancing. The UCOPIA Web Services platform is presented with all its functions and services. Finally, a summary of the different lines of product including their functionalities and objectives.

2 UCOPIA overview

UCOPIA offers security appliances dedicated to mobility management of wired and wireless networks. The main benefits of UCOPIA are:

- **Corporate and users' security: UCOPIA provides robust mutual authentication based either on a Web based, secure HTTPS portal or an industry compliant 802.1x architecture including a RADIUS server. After authentication, the communications confidentiality is guaranteed based on third party encryption such as VPN or Wi-Fi access point WPA/WPA2. An authentication method based on HTTPS and a Web-portal (login and password) is also offered to allow unrestricted network access provisioning for guests. Once authenticated, UCOPIA grant and enforce to each user or group an access rights profile. A user profile defines which applications are allowed, also taking time and location into account. Last, connection data (who did what when) is stored in a database for audit or legal issues.**
- **End user ease of use and productivity: Mobile users very often face problems to connect with their laptop and access their applications outside of their own office. Getting an IP addressing, finding the Internet through proxies and firewall, using printers require awkward and time consuming configuration. With UCOPIA, no need to reconfigure the laptop. The UCOPIA controller automatically routes the user Internet traffic or access to corporate applications through the local infrastructure.**
- **Easy integration in corporate network. Organizations have a legacy network and security environment (DHCP, DNS, VLAN, VPN, directory, firewall, etc.). The Wi-Fi has to fit smoothly into this existing environment. UCOPIA has a very modular, extensible architecture enabling flexible, simple integration and interoperability with the corporate legacy network. Thus, organizations can deploy Wi-Fi as an extension of their existing LAN without reconsidering their existing architecture.**
- **Easy to install and operate: The UCOPIA box is very simple to install and configure thanks to its user-friendly administration tools. Creating profiles and user accounts can be carried out by non-specialist users. UCOPIA thus combines business-level security with exceptionally straightforward implementation.**
- **ROI of Wi-FI infrastructures: Organizations deploying Wi-Fi networks want a return on investment of their infrastructure. The UCOPIA Analytics service will enable organizations to better understand the uses and to better know their users. Used in conjunction with the Web Marketing Campaigns service, it is possible to provide users with value-added services generating additional revenue, and / or monetize access by adding targeted ads.**
-

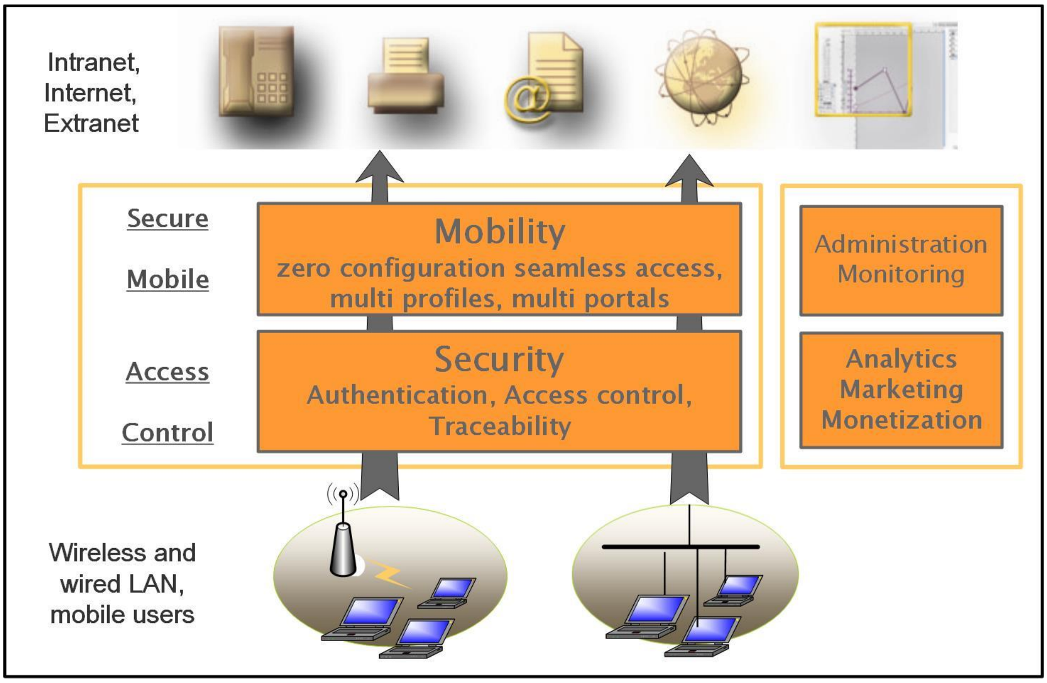


Figure 1: The UCOPIA solution

2.1 Global architecture

UCOPIA is a hardware (or virtual) appliance which controls connections and traffic on a wired (industry Ethernet cable and switches, eventually CPL equipments) and/or wireless (802.11 Wi-Fi Access Points) network infrastructure. This infrastructure is connected to an internal and secured network through the UCOPIA appliance that plays the role of a gateway as described by the following schema.

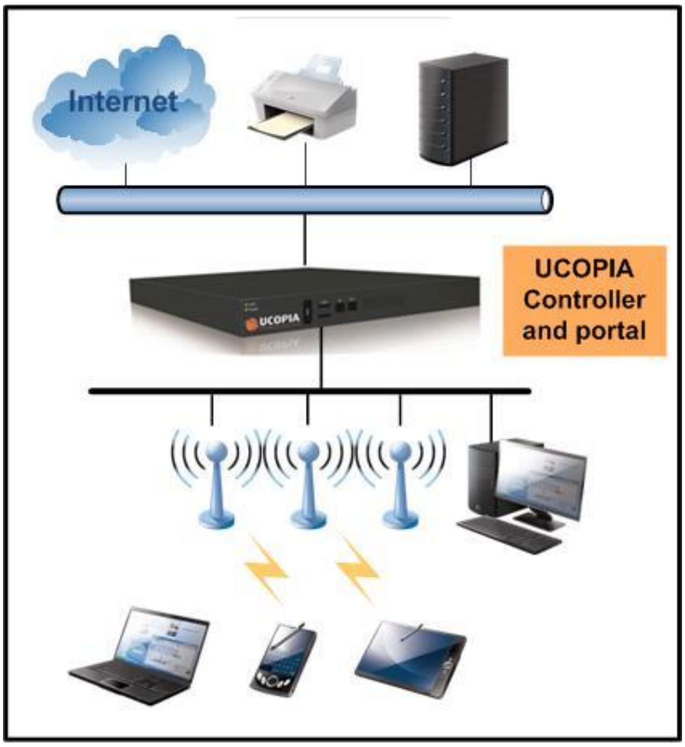


Figure 2: Global architecture

Other architectures are also possible, such as Cloud architecture, see Section 6.4.

The UCOPIA box comprises two main components:

- **The Controller implements robust and flexible authentication based on either a Web based HTTPS portal or a more robust 802.1x & RADIUS architecture. With the traffic filter included in the controller, user traffic is controlled based on user access rights granted. The controller automatically detects misconfigured network packet and fix the problem seamless. Thus, users get an unbeatable zero configuration access to network applications (internet, email, printers, etc.). Last, the controller manages the bandwidth and quality of service delivered to each user based on corporate policies. To face large deployments, UCOPIA controllers can operate in redundant or load balancing clusters.**
- **The Administration tool is a set of Web based tools in charge of the administration, configuration and supervision. The Manager enables the definition of services, users and groups, and related mobility policies (who is allowed to do what, where and when). With the manager, policies are centrally defined and stored in a corporate (LDAP) directory to be used by controller(s) when the user connects to the WLAN. The manager can also create delegation account, with privileged rights, allowing delegated users to create accounts with a simple and restricted web interface (example: Provisioning of accounts to welcome guests in a hotel or clients in a company).**

3 UCOPIA features

3.1 Security

Security is a requirement for mobile users. UCOPIA enables organizations to deliver enterprise class security and create the conditions for mutual trust between users and infrastructures.

The UCOPIA solution enables users to connect completely securely, thanks to its authentication mechanisms. Once connected, users can only access applications that are listed in their profile. This list of application may depend on the time and location. UCOPIA also enhances confidentiality by isolating users' traffic on different VLAN based on profile and usage.

3.1.1 CSPN security certification

UCOPIA has obtained CSPN (first level security certification) issued by ANSSI (the French Network and Information Security Agency). The certification confirms that the product has successfully passed a limited, fast-track evaluation run by an ANSSI-approved evaluation centre leading to certification.

The purposes of the evaluation work were to:

- **check that the product complies with its own security specifications (authentication, profile-based access controls, traceability, etc.);**
- **rate the mechanisms theoretically, and list the known vulnerabilities for products in its category;**
- **run vulnerability tests on the product intended to by-pass the security functions.**
-

See the ANSSI website to see the certification report.

http://www.ssi.gouv.fr/uploads/IMG/cspn/anssi-cspn_2010-01fr.pdf

-

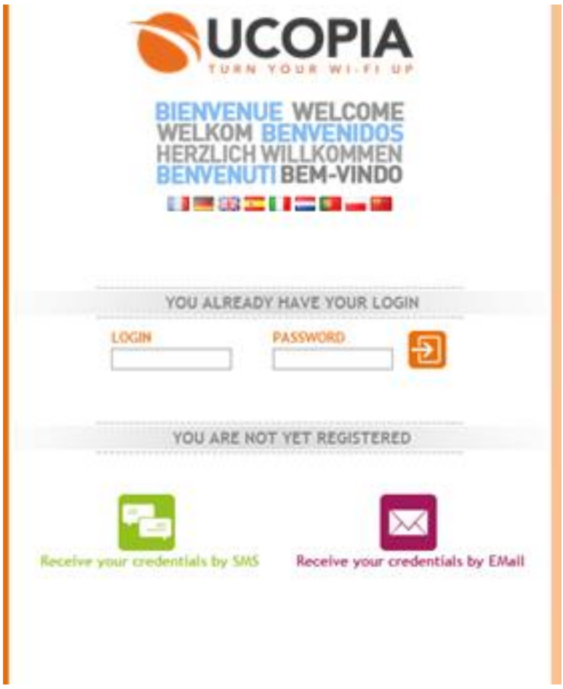
3.1.2 Authentication

UCOPIA proposes several ways to authenticate based on a RADIUS server running in the controller. One way to authenticate with UCOPIA relies on a Web browser on the user side, a captive portal in the UCOPIA controller and a secure HTTPS protocol. These different authentication methods co-exist within one network, possibly under different logical networks (VLANs), each corresponding to a different category of user. For example, a business might offer its employees strong authentication based on EAP-TLS certificates, and might reserve authentication by login and password from a Web portal for guest users. Within each authentication method, the authentication key has a limited lifespan.

3.1.2.1 Authentication with a Web portal UCOPIA

Authentication with a Web portal is very convenient to host guests since it does require any prior configuration or installation on the user laptop. The user opens a web browser on the terminal and is automatically redirected to an authentication Web portal embedded in the UCOPIA Controller (or possibly hosted elsewhere). The user enters the login name and password (standard mode) and if authentication is successful, the portal then shows the user which services are authorized.

The screenshot below shows the UCOPIA portal homepage enabling authentication by login and password (standard method) together with email or SMS authentication.



BIENVENUE WELCOME
WELKOM BENVENIDOS
HERZLICH WILLKOMMEN
BENVENUTI BEM-VINDO

YOU ALREADY HAVE YOUR LOGIN

LOGIN
PASSWORD

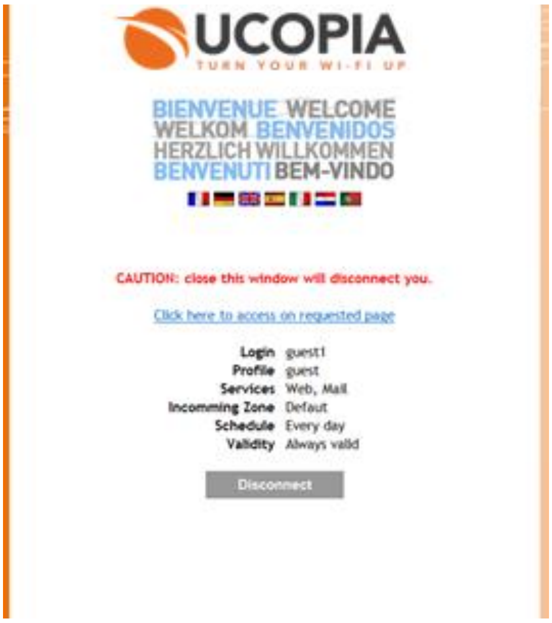
YOU ARE NOT YET REGISTERED

Receive your credentials by SMS

Receive your credentials by EMail

Figure 3: UCOPIA portal homepage

Once users are authenticated, the services authorized by their profile are displayed in the window.



BIENVENUE WELCOME
WELKOM BENVENIDOS
HERZLICH WILLKOMMEN
BENVENUTI BEM-VINDO

CAUTION: close this window will disconnect you.

Click here to access on requested page

Login guest1
Profile guest
Services Web, Mail
Incomming Zone Defaut
Schedule Every day
Validity Always valid

Figure 4: Display of authorized services from the UCOPIA portal

Automatic re-authentication

By default, UCOPIA provides mechanisms allowing to enforce security when using the portal. The security is offered by replaying the authentication periodically and transparently for the users. In this case, the users will have to keep the window of the navigator in order to stay connected. It is possible to disable this security option by just configuring the users' profiles. In this case, the users are going to be disconnected by turning of its network and shutting down its computer. The idle time is configurable.

Using the same login and password for multiple concurrent connections

By default, the same login/password cannot be used for two concurrent connections, for security and traceability reasons. This option can be unlocked in order to authorize multiple user connections with the same credentials. It is possible to customize the number of connections per users' profile.

Corporate portal redirection

The UCOPIA controller redirects the user at connection time on an external corporate portal. This method may be of interest when populating a marketing database, for example. As regards user authentication, two methods are on offer, namely (1) returning to the UCOPIA portal or (2) remaining on the corporate portal which then needs to have the UCOPIA authentication dialog added. For this last case, UCOPIA supplies an API enabling the authentication dialog to be run.

3.1.2.2 Social networks authentication

In order not to increase the number of identifiers for users and thus simplify use, the user can use the identifiers of one of his social networks (Facebook, Twitter, Google, LinkedIn) to authenticate to the captive portal.

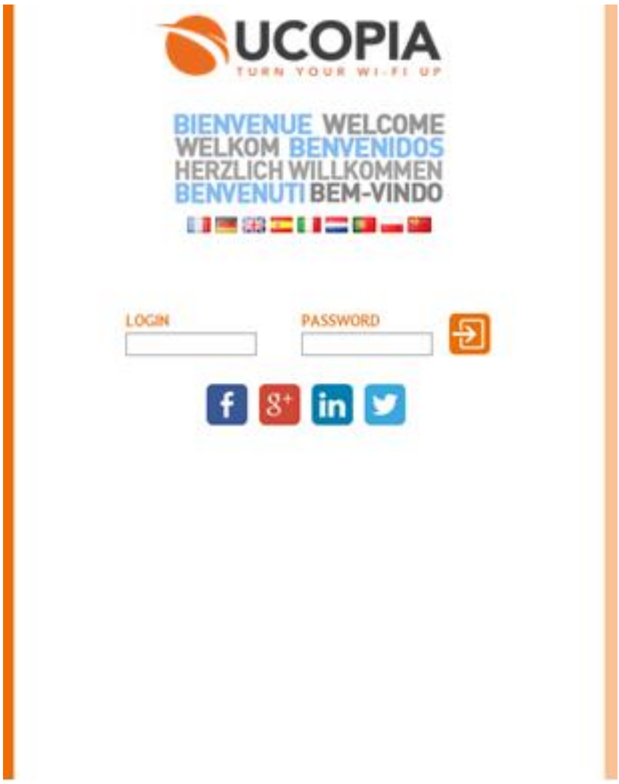


Figure 5: Social Networks authentication

The user connecting via Twitter on the captive portal can become, with a single click, a "Follower" of a given Twitter account. One who uses Facebook will be able to post a "Like".

Information coming from the end-user is registered in the UCOPIA logs for traceability and/or marketing purpose. The following information will be exploitable according to the social networks, the name, first name, email, birthday, gender, and prefered language. They can in particular be used by Analytics tools (see Section 8.2). The agreement of the use of personal information for marketing purposes can be controlled by a charter, its acceptance or its refusal is stored into the user logs (opt-in marketing).

A new corporate social application can be developed by the organization deploying UCOPIA in order to provide a branded page when entering credentials.

3.1.2.3 OpenID Connect authentication

OpenID Connect is an identity layer which allows to verify the identity of an end-user based on the authentication performed by an authorization server.

It can be used to implement SSO mechanisms (Single Sign On) to unify and minimize authentication requests. For example, to authenticate using credentials of the tax authority website (login and password) on the town hall's website.

OpenId Connect allows to easily interoperate with solutions such as Instagram or Office 365.

3.1.2.4 RADIUS/802.1x authentication

A RADIUS server is embedded in the UCOPIA controller, it allows to manage the authentication server for 802.1x authentication protocol.

Authentication with login & password and 802.1x protocol

A secure login/password solution is available based on PEAP (natively supported by Windows environments) and TTLS (Linux & Mac OS X platforms). This requires a very simple one time configuration of the user terminal while delivering robust, industry standard mutual authentication.

Certificate authentication with 802.1x

Authentication with certificates is based on an EAP/TLS protocol. Certificates are managed by a Private Key Infrastructure (PKI) which creates, revoke, stores and distributes certificates. Both the UCOPIA controller and the user get a certificate from the same PKI. UCOPIA makes use of certificates issued by a trusted third party. This authentication method offers a compromise between security and ease of deployment.

3.1.2.5 Automatic authentication based on MAC address

After a first successful authentication to the portal, UCOPIA can record the MAC address of the user. This makes it possible to seamlessly connect the user when they try to log on in the future, thanks to the automatic recognition of their MAC address.

This mechanism provides a smoother customer experience by presenting the authentication portal only when the user first connects to the system. The activation of this mechanism is done at the level of the user's profile and it can be applied to any type of portal.

In addition, it is possible to lock access for a given device (or more) from its MAC address. This prevents password sharing among multiple users using different equipment.

3.1.2.6 Authentication based on fixed MAC address or IP address

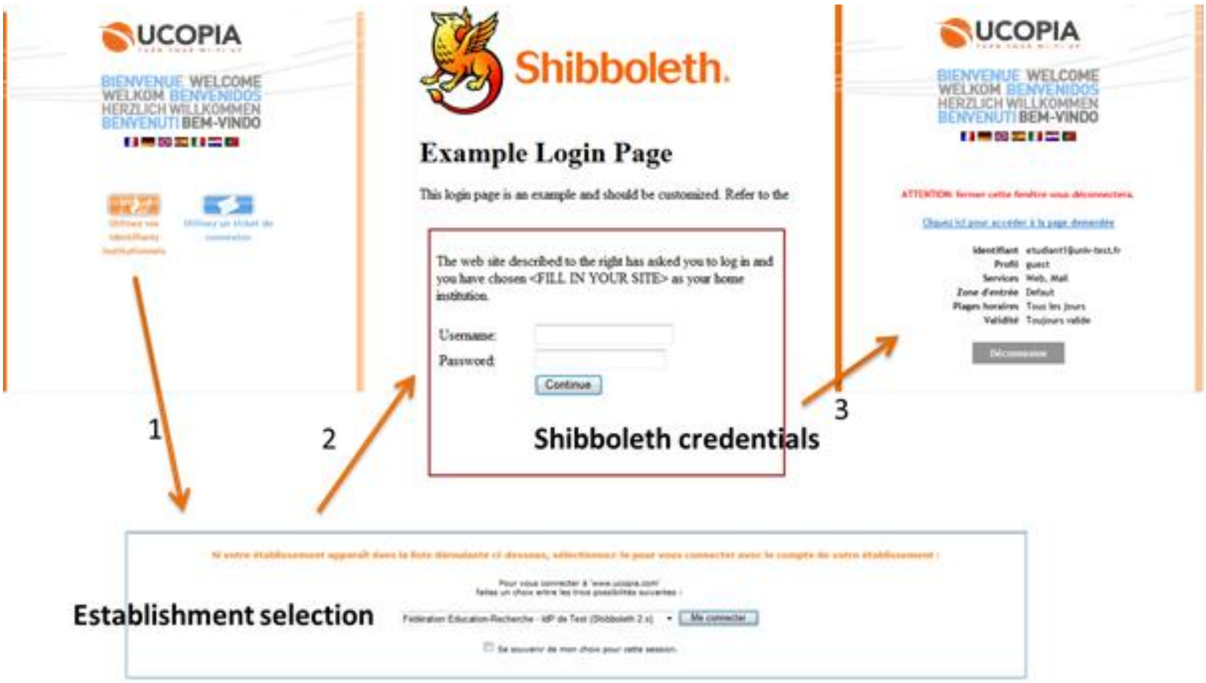
UCOPIA also offers authentication based on the MAC or IP address. This method may prove useful for authenticating IP devices which might not have the capability to be authenticated with more advanced protocols such as 802.1x.

3.1.2.7 Windows environment authentication

UCOPIA can be used in a Windows environment to authenticate machines before user authentication. The purpose of machine authentication, beyond its prime function of authentication, is to allow scripts (such as Netlogon) to be run on the Windows server which will, for example, mount network drives, execute anti-virus update scripts, start up certain special utilities, etc.

3.1.2.8 Shibboleth authentication

Shibboleth is an identity propagation mechanism deployed in university environments in particular. The aim is to enable the user to be able to authenticate themselves with their Shibboleth credentials from UCOPIA's captive portal. To this end, the user is redirected to a page that allows them to first select their home institution, and then enter their login credentials (see Section Shibboleth architecture for the technical architecture).



Example Login Page

This login page is an example and should be customized. Refer to the

The web site described to the right has asked you to log in and you have chosen <FILL IN YOUR SITE> as your home institution.

Username:

Password:

Continue

ATTENTION: fermer cette fenêtre vous déconnectera.

Cliquez ici pour accéder à la page demandée

Identifiant	etudiant1@univ-test.fr
Profil	guest
Services	Web, Mail
Zone d'entrée	Defaut
Plages horaires	Tous les jours
Validité	Toujours valide

Déconnexion

Si votre établissement apparaît dans la liste déroulante ci-dessous, sélectionnez-le pour vous connecter avec le compte de votre établissement :

Pour vous connecter à 'www.ucopia.com'
faites un choix entre les trois possibilités suivantes :

Fédération Education-Recherche - IdP de Test (Shibboleth 2.x) Me connecter

□ Se souvenir de mon choix pour cette session.

Figure 6: Shibboleth authentication

3.1.3 Access Control based on user profile

The user profile describes the access rights to the applications, the duration and the connection mode, time slots and authorized zones of connection, etc. A user can have multiple profiles depending on different criteria (location, time, equipment).

Once authenticated, the user profile is downloaded from the corporate directory in the UCOPIA controller which compiles this profile into a set of multi-level traffic and routing rules, based on IP address, port, protocol, URL, IP address, etc. The UCOPIA filtering engine then analyses user traffic and removes forbidden access.

3.1.4 Connections traceability and logs

UCOPIA records and logs 2 kinds of information: session information (who connected where and when) and traffic information (who did what). **In most European countries, in the context of anti terrorism laws, delivering Internet access to guests require 12 months traceability** (see Section 3.5.3).

3.1.5 VLAN Management

UCOPIA enables to manage Virtual Networks (VLANs) both on the user and the LAN sides. VLANs are part of the legacy network infrastructure for security and management purpose. VLANs are used to insulate different populations of users in different virtual networks.

Based on user identity, users are mapped into a specific VLAN. Users in the same VLAN or different VLANs can be insulated or see each other. This complements the encryption features to deliver either confidentiality or allows work group. UCOPIA provides a flexible way to define and map access VLANs where the user connect and applications VLANs where corporate applications and services are available, and define an IP addressing scheme for each of this VLANs. On each access VLAN, UCOPIA maps a specific set of IP addresses. UCOPIA works both in NAT mode and in Router mode depending on VLAN and user profile (see IP addressing and VLANs architecture section).

Depending on profile, the user traffic can be forced by the UCOPIA controller on a specific application VLAN (for instance guest's traffic is forced on a VLAN where only Internet access is available).

Schema below illustrates a network architecture using 3 isolated access VLANs (Administration, Web portal & 802.1x/EAP). Visitors authenticate using the web portal and the employees using 802.1x. Each population is redirected to the appropriate outgoing VLAN depending on their profile.

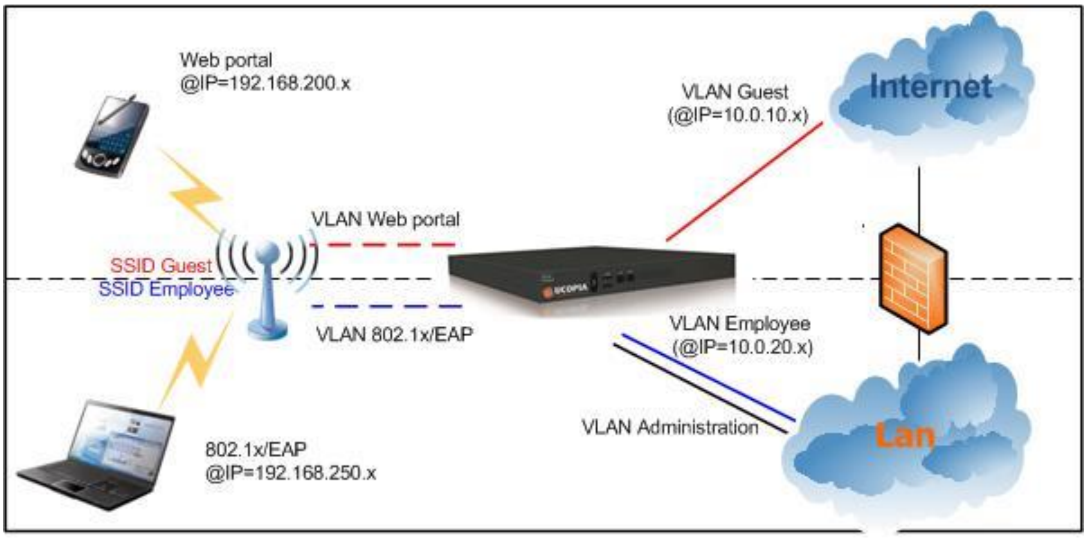


Figure 7: UCOPIA VLAN architecture

3.1.6 URL filtering

UCOPIA provides a native URL filtering mechanism. Filtering can be applied as user profile level. Several URL categories are available (Adult, Aggressive, etc.) allowing to apply different policies and to differentiate for example an "Adult" profile from a "Child" profile.

The available categories are the following:

Adult	Adult sites from erotic to pornography.
Advertising	Advertising sites.
Aggressive	Aggressive sites.
Bank	Online banking sites.

Blog	Blog hosting sites.
Chat	Various chat sites.
Dating	Online dating sites.
Drugs	Sites relative to drugs.
File hosting	File hosting sites.
Gambling	Online gambling sites.
Hacking	Hacking sites.
Malwares	Sites hosting malware programs.
Online games	Online gaming sites.
Phishing	Phishing sites.
Press	Online press sites.
Redirector	Sites bypassing the URL filtering system.
Shopping	Online shopping sites.
Social networks	Social networks.
Video	Audio and/or video hosting sites.
Warez	Sites that host a list of links to download files.
Webmail	Webmails.

New categories can be added very easily. For each category it is possible to specify whether it is a permitted or prohibited category. The order of the categories when filtering can also be configured. It will, for example, possible to add a category to allow only the use of intranet sites, or for business purpose to prohibit sites of its competitors.

Domains of HTTPS URLs are taken into account by the filtering mechanism.

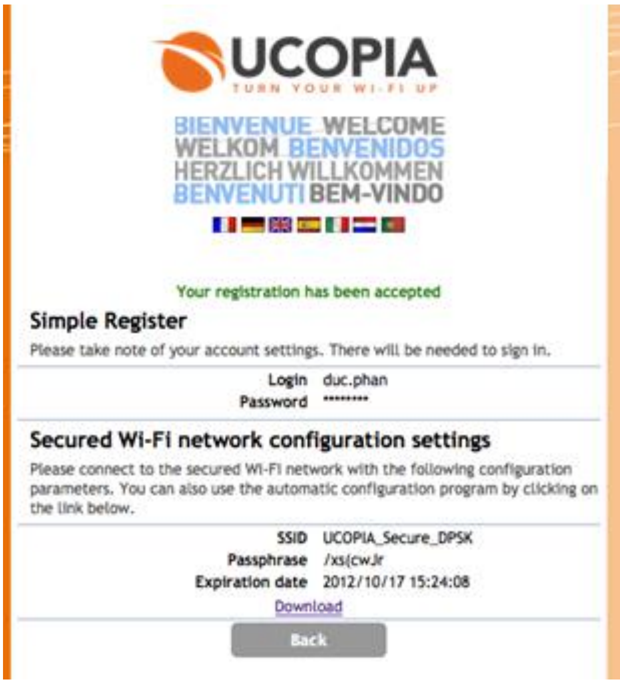
It is also possible to use an external filtering tool either through the ICAP protocol or by using an HTTP traffic redirection. Redirection works by means of a Web proxy embedded in the UCOPIA controller. It is possible firstly to redirect traffic to the URL-filtering product, and secondly to communicate user-related data (login and password) to it. This makes it possible for the filtering product to apply different policies depending on the user.

3.1.7 DPSK (*Dynamic Pre Share Key*) Ruckus

The Ruckus[1] Wi-Fi solution offers an innovative mechanism for dynamically distributing encryption keys, generating a unique key per user. DPSK is an ideal compromise between 802.1x and simple passphrases.

UCOPIA's captive portal may be associated with the DPSK mechanism in order to strengthen portal security while maintaining ease of use.

The user will firstly be associated with an open SSID and register on the UCOPIA portal by using one of the self-registration methods available. The key will be assigned and transmitted to the user at the same time as their credentials. A utility program can be downloaded from the portal for automating the configuration of the key for their particular equipment. The user can then log on to the portal with their credentials; they will be associated with a secure SSID and their traffic will be encrypted.



Your registration has been accepted

Simple Register

Please take note of your account settings. There will be needed to sign in.

Login duc.phan
Password ********

Secured Wi-Fi network configuration settings

Please connect to the secured Wi-Fi network with the following configuration parameters. You can also use the automatic configuration program by clicking on the link below.

SSID UCOPIA_Secure_DPSK
Passphrase /xs(cwJr
Expiration date 2012/10/17 15:24:08

Figure 8: UCOPIA portal with Ruckus DPSK

3.1.8 Intrusion detection

UCOPIA detects and neutralizes attacks consisting in stealing the identity of a user terminal or the identity of the UCOPIA controller. This mechanism consists on taking the MAC address from an authenticated machine and using it as its own. From a technical perspective, this means UCOPIA detects level 2 intrusions such as ARP poisoning. Once detected, UCOPIA resets the ARP table to neutralize the attacks. ARP poisoning is very important in particular when the authentication mode is not 802.1x.

In this case, unknown users (eventually hackers) could get an IP address before authentication and could launch an attack without authenticating via the WEB portal.

[1] www.ruckuswireless.com

3.1.9 Encryption

Data that circulates on the network, in particular on the Radio frequencies should be encrypted for confidentiality purpose. Equipment manufacturers delivered different types encryption solutions: TKIP and lately 802.11i AES based encryption, WPA, WPA2, VPN, etc. 802.11i is robust enough for most users but it requires that both the infrastructure and the user terminal are 802.11i compliant. To enable organizations to deploy and use WPA, the UCOPIA controller distributes encryption keys to the authenticated users automatically. UCOPIA complies with all these solutions and industry standards.

3.1.10 Audit logs

For purposes of safety and traceability, all management operations are recorded in Syslog format. This includes transactions from the administration tool, the portal delegation and CLI.

3.2 Mobility

Mobility management means the definition of corporate policies handling various situations (which applications or resources are needed by employees within their office, in a meeting room, at the cafeteria, which services should be delivered to the visitors, whether customers, partners, etc.). Once corporate policies for mobility are defined, the next step is to make sure that users can seamlessly access to authorized services with appropriate. At last but not least, users share WLAN bandwidth and a poor bandwidth management means uncontrolled quality of service and poor user experience.

3.2.1 Mobility model

UCOPIA implements a rich and flexible mobility management model which takes into account “Who” can do “What”, “Where”, “When” and “How”. “Who” stands for users or group of users and their equipments. Users inherit access right from their group but customization is supported. “What” refers to all applications or resources (e.g. printers). “When” refers to the time or date (e.g.: Working day and working hours, meeting time, etc.). Furthermore, user rights may change depending on “Where” the user is (e.g.: In the office, a training room, lobby) based on the zone where the user connected. “How” includes considerations about bandwidth (e.g.: Which bandwidth to grant to a given user to use a given application), or security level (full encryption, tunnelling, open).

For instance, a user connecting from the headquarters of his company will connect using 802.1x, and will get access to the internal LAN of the company, all the time. If the same user tries to connect from a meeting room of a subsidiary, he might only get access to the Internet through an open network (and will only get access from 9.00 to 18.00).

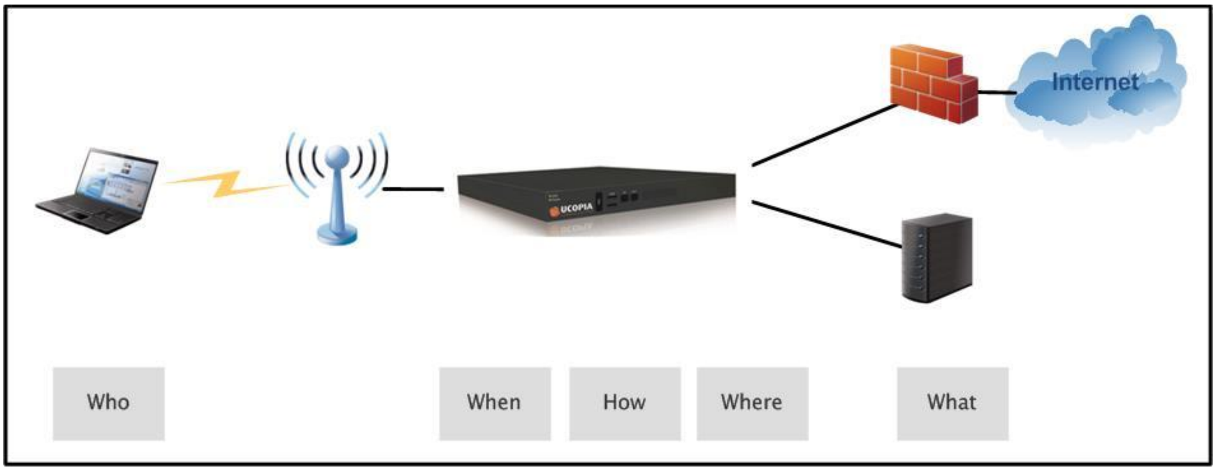


Figure 9: The UCOPIA Mobility model

3.2.2 Conditional & adaptative profile

With UCOPIA, the applicable profile for a user can change based on the connection location (branch office and headquarter), the zone (an area within a location), the date and the connection time and the type of equipment used for the connection.

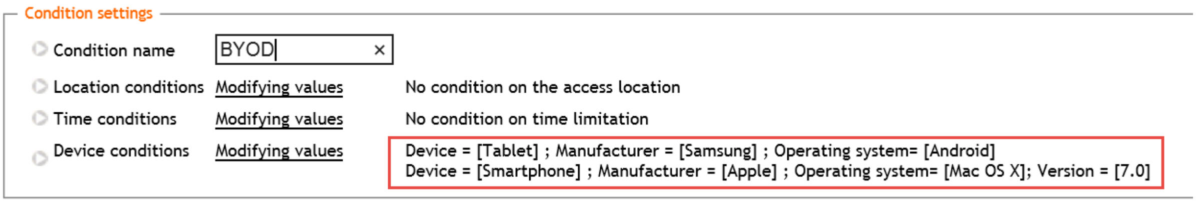
Thanks to adaptable profiles created by UCOPIA, the following scenarios can be implemented:

1. Students connecting from a lecture hall during the exam period will not get access to the Internet but only to the internal servers.
2. Students connecting from the library will get access to the Internet for 2 hours, but by connecting from their student rooms they will get an unlimited access to the Internet.
3. For guests in their hotel room, a wired access delivers triple play services including Internet access, telephony, video on demand and Pay TV.
4. Internet access is free of charge and unlimited. For hotel visitors (not having a room booked) and customers in the public areas (lobby, meeting rooms, restaurant), only internet access is available and charged based on connection duration.

3.2.3 BYOD (Bring Your Own Device)

Conditional profile can apply to the type of device of the user and allow to implement security policies and mobility in a particular type of equipment. This feature can be used in enterprises to manage BYOD and apply special treatment to employees personal equipment. For example, mobile phones and tablets will only connect to the working days and hours with restricted access rights.

When defining the profile, the condition BYOD can be expressed as follows:



Condition settings

○ Condition name BYOD ×

○ Location conditions Modifying values No condition on the access location

○ Time conditions Modifying values No condition on time limitation

○ Device conditions Modifying values Device = [Tablet] ; Manufacturer = [Samsung] ; Operating system= [Android]
Device = [Smartphone] ; Manufacturer = [Apple] ; Operating system= [Mac OS X]; Version = [7.0]

Figure 10 : BYOD conditions

If the condition is satisfied, the profile adapts to implement access rights and appropriate schedules connection.
It should be noted that the conditions for selecting equipment may involve the manufacturer and operating system (name and version).

3.2.4 Seamless Zero Configuration Access

Many Professional users spend most of their working time outside of their own office: working with colleagues, customers or partners in a meeting room, visiting branch offices, or worldwide subsidiaries, etc.

They use a laptop which works perfectly in their own office but they face various problems when connecting outside. This includes problems such as getting an IP address, accessing Internet through a proxy, using a printer, reading and sending email, or provisioning an account on a corporate PBX to use Wi-Fi smart phones. Configuring the user terminal back and forth can make user experience terrible and create a lot of stress for technical helpdesk. UCOPIA enables seamless, zero configuration access to network services and applications. The controller knows how each local application and service works. Based on its filtering engine, UCOPIA analyses user traffic (who the user is, what kind of application he/she is willing to access), understands what the user is willing to do, detects misconfigured flow and fix the configuration issues automatically.

- **IP addressing: The first configuration issue for mobile users is the way to get an IP address. Laptops are configured with various IP addressing schemes (DHCP, NAT, fixed) which do not complies with each other. With UCOPIA, the user does not need to care about getting an IP address and changing IP configuration. The UCOPIA controller fits in the middle and handles this question.**
- **Internet access: Many organizations have a Web proxy to secure and fasten corporate Web access. Accessing Internet through a proxy requires configuring the laptop browser application specifically and likely to get assistance from helpdesk. Any mobile user has to reconfigure the laptop browser configuration back and forth, causing waste of time and additional helpdesk workload. With UCOPIA, no need to reconfigure the browser. The UCOPIA controller dynamically routes traffic through the local proxy.**
- **Email: Reading and sending email is an issue for mobile users. This is because the mail application uses a corporate user mail account, and this account points to the corporate mail server. The mail server can be accessed locally when the user is connected on the corporate LAN and eventually remotely through a VPN. With UCOPIA, visitors outgoing emails are automatically detected and can be seamlessly redirected to a local mail server.**
- **Printing: Printing a document means identifying the appropriate printer (the one that is close to the user), and set all configuration and software required to use it: printer name and selection, driver installation, etc. With UCOPIA, the entire process is completely seamless: UCOPIA detects the print request, automatically installs the driver if needed, and prints the document.**

  UCOPIA is also compatible with the AirPrint[2] solution, for seamless printing in an Wi-Fi and Apple environment.

-

All of these mechanisms for transparency of access implemented by UCOPIA ensure productivity and ease of use for end users. It spectacularly reduces technical support's workload, as it is no longer necessary to ask for their help when connecting to a local environment.

-

[2] AirPrint is a type of technology developed by Apple that enables users to print high-quality documents, and which is based on Apple's printing architecture requiring no drivers.

3.2.5 Quality of Service

UCOPIA can differentiate between traffic flows through UCOPIA boxes and consequently manage traffic priorities on the basis of choices made by administrator.

Two levels of Quality of Service management are on offer:

- **QoS by service**
- **QoS by user**

3.2.5.1 QoS by service

For each service, it is possible to define:

- **Service based priorities**

  Services or services for a specific group of users can have 2 different levels of priority (normal and high). The UCOPIA filtering engine detects normal and high priority traffic and sorts the corresponding packets in different priority queues. For instance, guest internet traffic can get a normal priority while employee internet traffic gets high priority. Both guest and employees populations share the existing bandwidth but employees get a much larger bandwidth.

- **Guaranteed throughput**

  On top of the priorities feature, UCOPIA enables to set a guaranteed minimum bandwidth for a specific service. For instance, it is possible to set a minimum 30Kbs for a Voice over IP service.

  Transfer speed is expressed in kilobits per second (Kbps).

- **Bandwidth limitation**

  Bandwidth restrictions are applied to a service and are expressed in Kbps. Traffic packets exceeding this limit are removed.

3.2.5.2 QoS by user

A limit on upstream and downstream bandwidth can be set per user at user profile level. All users with that profile will be allocated these limits. The downstream bandwidth equates to the data flow in from the Ethernet IN to OUT; the upstream rate is the opposite.

3.2.6 Data volume quota

To control the use made of the network, a quota volume of transferred data can be defined at the user's profile level. This quota may be set for the upload flow, download flow or the sum of both. If the threshold is exceeded, rules may apply to either block the user or limit his bandwidth

-

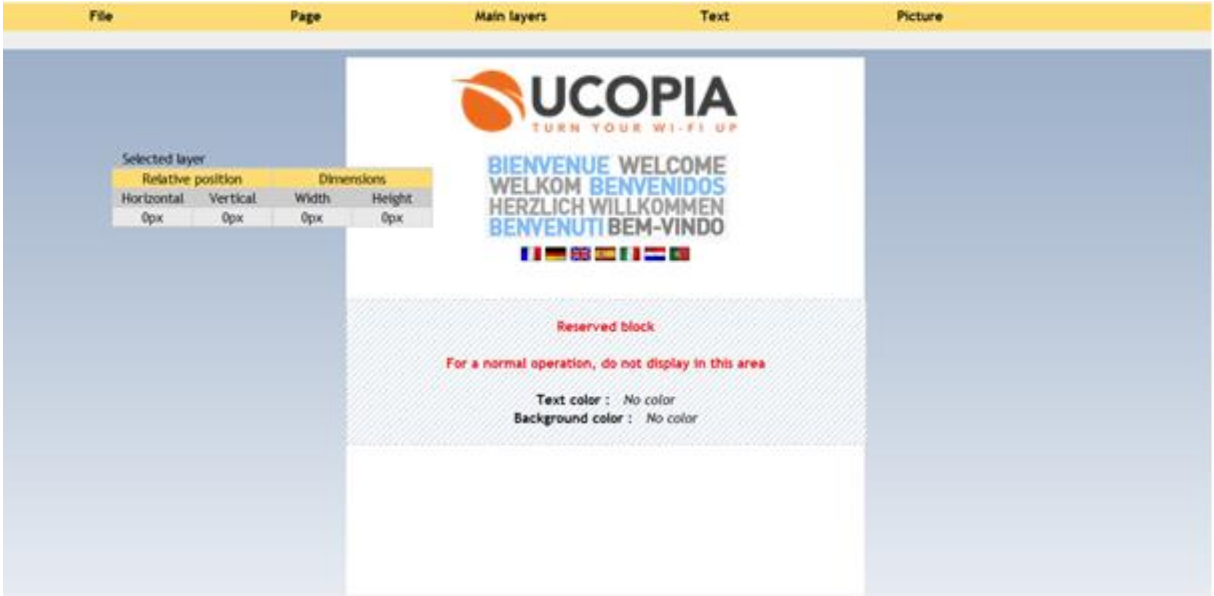
3.2.7 Multiple portals

The different portal modes can be used at the same time. Indeed, for each incoming zone a portal can be created (see Section 6.3) with multiple modes. For example, in a hotel, clients can register using SMS, for a connection limited to one hour, and hotel customers can get an unlimited access created with a PMS with unlimited connection time.

3.2.8 Portal customization

This portal can be customized with a WYSIWYG portal editor, allowing logo, banners, message and links to be changed very easily.

The screenshot below shows the portal in WYSIWYG “Edit” mode.



Selected layer

Relative position		Dimensions	
Horizontal	Vertical	Width	Height
0px	0px	0px	0px

Reserved block

For a normal operation, do not display in this area

Text color : No color
Background color : No color

Figure 11: The UCOPIA portal editor

For more advanced customization, the portal's HTML code can be exported, amended and re-imported into the UCOPIA controller.

The portal can be designed for different formats such as laptop, smartphone or tablet. 15 languages are available.

3.2.9 Captive portal and advertising

The UCOPIA captive portal is able to display dynamic content (text, images, video) from a content server.

Using this feature, the UCOPIA portal can display dynamic content coming from an advertising agency, each portal refresh will propose a new advertising.

The following screenshot shows an example of customized portal including advertising.

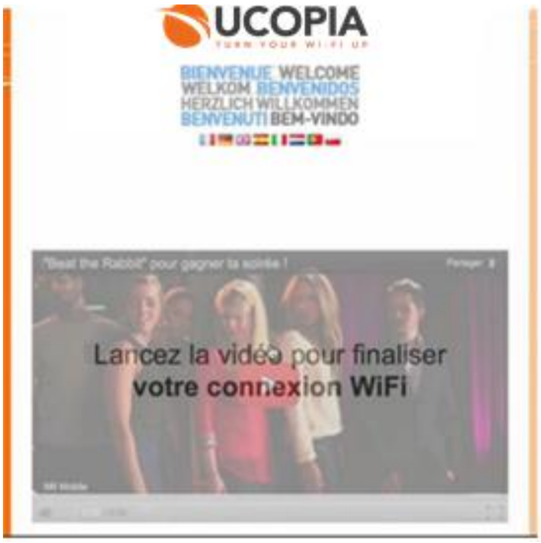


Figure 12: Customized UCOPIA portal with advertising

3.2.10 Smartphone App

A UCOPIA Smartphone App is available. The application serves two purposes: firstly it simplifies connection to a UCOPIA network, and secondly it allows trough administrators to create user accounts very simply.

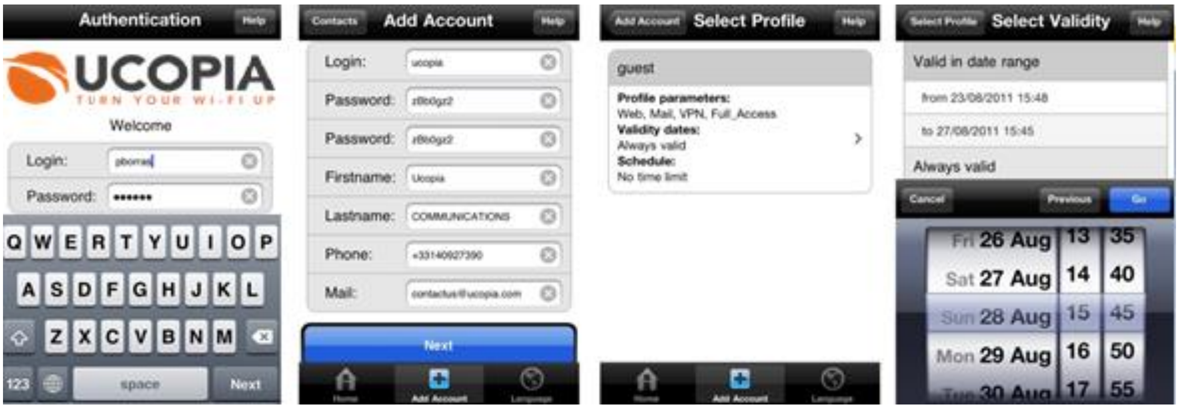
The Smartphone application provides a self-registering mode. This mode avoids creating a user account from the captive portal. At the first user connection, the user is asked to fill a form, other connections are seamless access. Optionally, the form can be skipped for a fully transparent access.

The Smartphone application stores the user's login and password, which are automatically retrieved when UCOPIA requests authentication.

User accounts can be directly created from contacts in the Smartphone contact list, and connection tickets can be sent to the user from the Smartphone by SMS or email.

The application can be customized (logo, text).

The Smartphone App is free of charge, available for iPhone, Androïd and BlackBerry in French or English.



Login: pborrel
Password: ••••••

Login: ucopia
Password: z8b0gz2
Password: z8b0gz2
Firstname: Ucopia
Lastname: COMMUNICATIONS
Phone: +33140927390
Mail: contactus@ucopia.com

guest
Profile parameters:
Web, Mail, VPN, Full_Access
Validity dates:
Always valid
Schedule:
No time limit

Valid in date range
from 23/08/2011 15:48
to 27/08/2011 15:45
Always valid

Fri 26 Aug 13 35
Sat 27 Aug 14 40
Sun 28 Aug 15 45
Mon 29 Aug 16 50
Tue 30 Aug 17 55

Figure 13: UCOPIA Smartphone App for iPhone

3.2.11 iPass Compatibility

iPass[3] is a solution that allows mobile users to securely connect to their professional environment using a Wi-Fi infrastructure. iPass can be used from a PC, smartphone, or tablet.

The UCOPIA solution is compatible with iPass, processing all iPass users seamlessly. This is an advantage for any organization (hotels, convention centers, etc.) that wants to attract and increase customer loyalty for its professional users (see Section 5.7.4 for more details).

3.3 User account provisioning

Accounts can be created in different ways: by the administrator, using the administration tool; on the delegation portal, by a delegated administrator; and by the end user, through the self-registration methods of the captive portal.

[3] www.ipass.com

3.3.1 Self-registering from the captive portal

Different modes of self-registration are provided. These modes are available from the captive portal and can potentially coexist as options. For example, it is possible to set up a portal that combines the standard mode (login/password) with one or more self-registration modes (SMS, email, etc.).

The advantage for providing the account through self-registration is that it requires no intervention from administrators, since the user account is automatically created by the self-registration action. To enhance security, you can add a password request prior to allowing access to the portal; this password will be the same for all users of the portal.

3.3.1.1 "One-Click Button"

The "One-Click Button" portal was designed to provide significant ease of use. It is based on a one-button connection to access the services. This portal can be complemented by a charter acceptance request or a form requesting information.

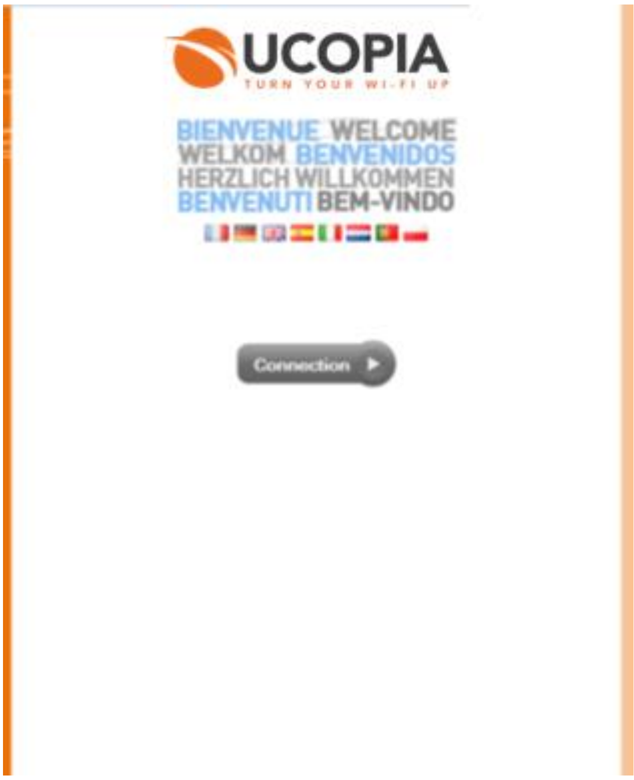
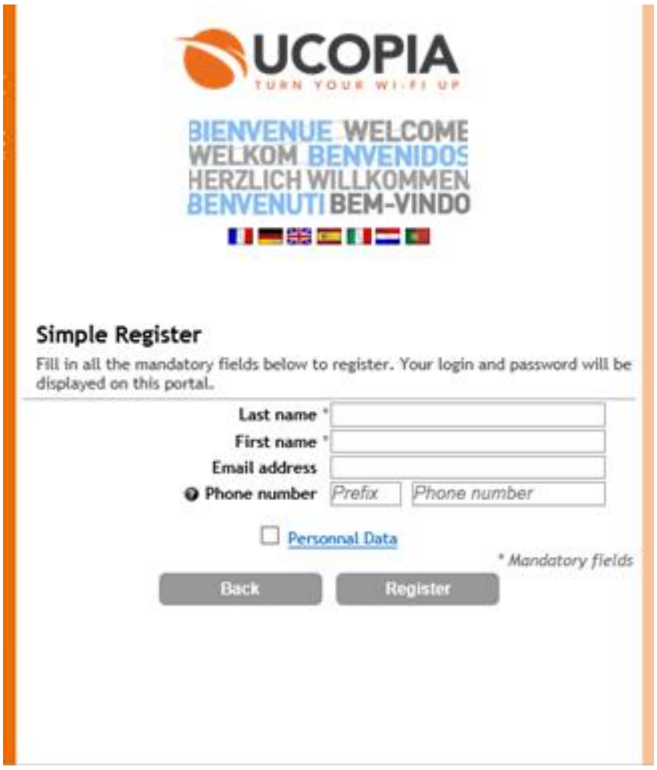


Figure 14: The "One-Click Button" Portal

3.3.1.2 Open registration

Users register on the portal by giving their surname, first name and possibly email address and telephone number. They receive a login and password directly on the portal. The advantage of this method is that ease of use is given priority.



Simple Register

Fill in all the mandatory fields below to register. Your login and password will be displayed on this portal.

Last name *
First name *
Email address
Phone number Prefix Phone number

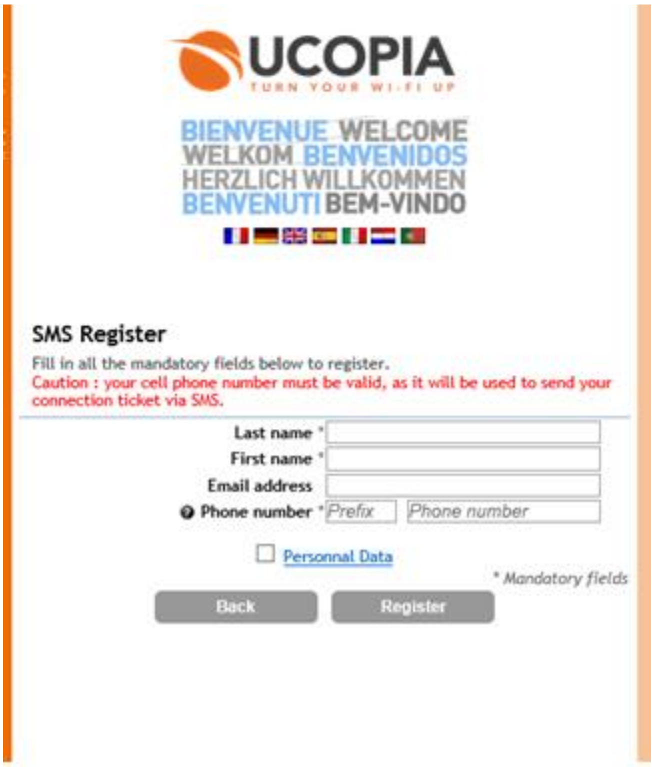
□ Personnal Data

* Mandatory fields

Figure 15: Portal with self-registration using a form (form is filled by user)

3.3.1.3 SMS registration

The end user opens the WEB browser, hits the UCOPIA portal, and types her/his name and cell phone number. A password is automatically generated by UCOPIA and sent to the user in a SMS on his cell phone. To use this mode, the organization using the UCOPIA solution just has to create an account to one of the many SMS gateways and sending platform proposed by UCOPIA (Orange, TM4B, and SMTP to Text solutions). Traceability is guaranteed by the customer’s mobile phone number.



BIENVENUE WELCOME
WELKOM BENVENIDOS
HERZLICH WILLKOMMEN
BENVENUTI BEM-VINDO

SMS Register

Fill in all the mandatory fields below to register.
Caution : your cell phone number must be valid, as it will be used to send your connection ticket via SMS.

Last name *	
First name *	
Email address	
Phone number *	Prefix Phone number

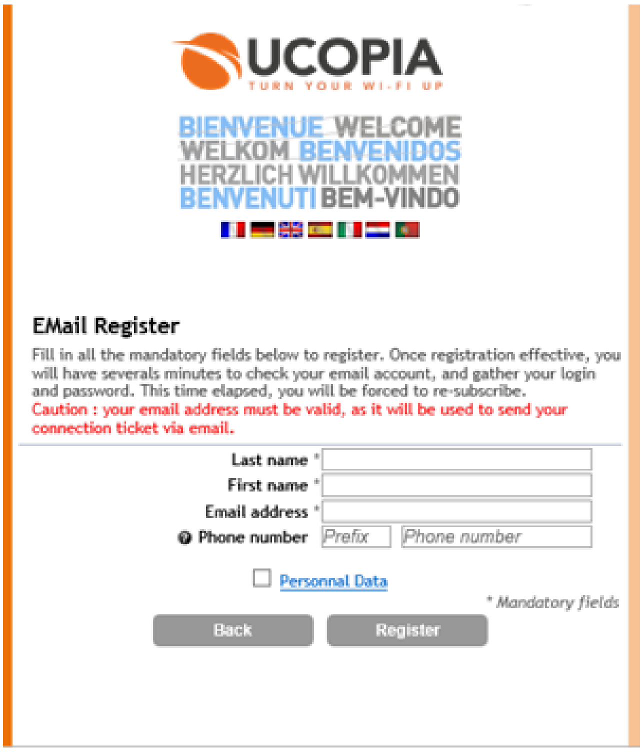
□ Personnal Data

* Mandatory fields

Figure 16: Portal with self-registration by SMS

3.3.1.4 Email registration

The users register themselves on the portal. They have to provide their first name, last name and email address. They will receive a password and login by mail. To allow this kind of authentication method, the administrator has to allow a user to connect for a limited period of time to allow a user to get access to his mailbox. Traceability is provided through the user's email address. As with SMS registration, the main advantage of this method is that there is no need for an administrator to create the user's account, the account being created automatically by self-registration. It also has the benefit of being free of charge, whereas the SMS method has the cost of a text message.



EMail Register

Fill in all the mandatory fields below to register. Once registration effective, you will have severals minutes to check your email account, and gather your login and password. This time elapsed, you will be forced to re-subscribe.
Caution : your email address must be valid, as it will be used to send your connection ticket via email.

Last name *
First name *
Email address *
Phone number Prefix Phone number

□ Personnal Data

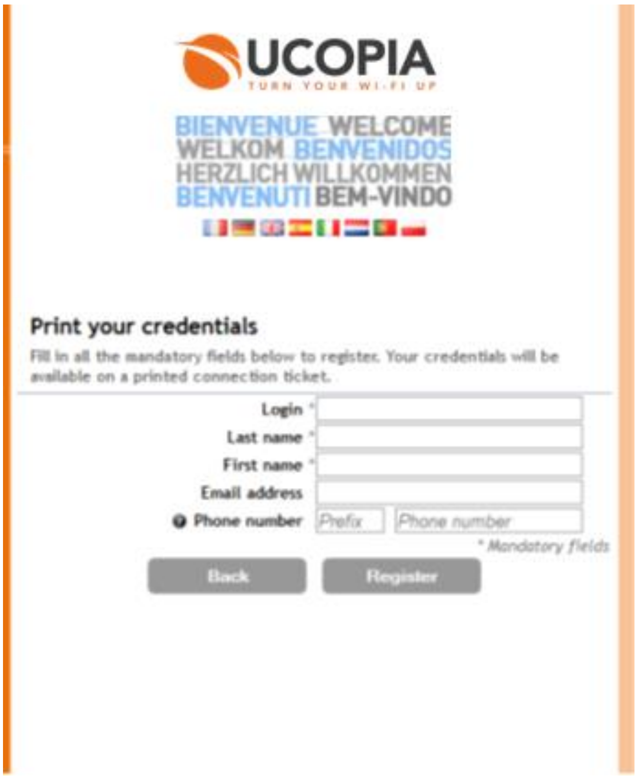
* Mandatory fields

Figure 17: Portal with email self-registration

In this mode, the email domains can be controlled in order to authorize or prohibit certain domains. For example, it’s possible to avoid "garbage" emails and / or restrict the use of the portal to users whose domains are known (e.g, partners, suppliers). It is also possible to assign a different user profile according to the domain.

3.3.1.5 Self-registration by ticket printing

In this case, the user performs their registration on the UCOPIA portal by completing a form and then printing a ticket that will list their credentials. The ticket is printed at the reception of the organization where the person is using the system. This mode has the advantage that it saves a considerable amount of time for the receptionist (no information to be entered) and it provides a secure connection (the user must report to the reception to get their credentials, where an identity check may be performed if desired).



Print your credentials

Fill in all the mandatory fields below to register. Your credentials will be available on a printed connection ticket.

Login *	
Last name *	
First name *	
Email address	
Phone number	Prefix Phone number

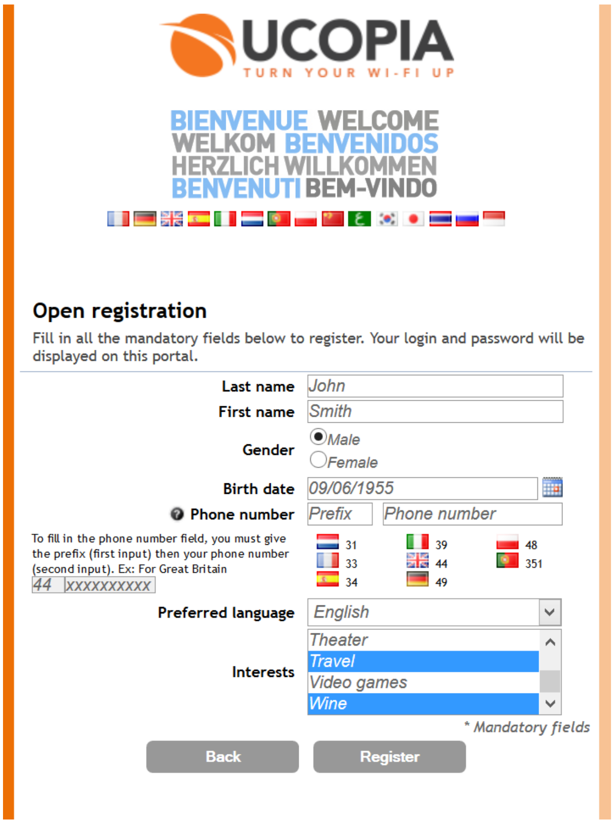
* Mandatory fields

Figure 18: Portal with self-registration by ticket printing

3.3.1.6 Personalized form to collect user data

The modes with self-registration can be enhanced with input form to collect information on the person who is logging on.

Information such as name, email address, phone number, gender, date of birth, interests, etc. can be requested mandatory or optional basis.



Open registration

Fill in all the mandatory fields below to register. Your login and password will be displayed on this portal.

Last name	John
First name	Smith
Gender	● Male ○ Female
Birth date	09/06/1955
Phone number	Prefix / Phone number
To fill in the phone number field, you must give the prefix (first input) then your phone number (second input). Ex: For Great Britain 44 xxxxxxxxxx	31 33 34 39 44 49 48 351
Preferred language	English
Interests	Theater Travel Video games Wine

* Mandatory fields

Figure 19 : Example of personalized form

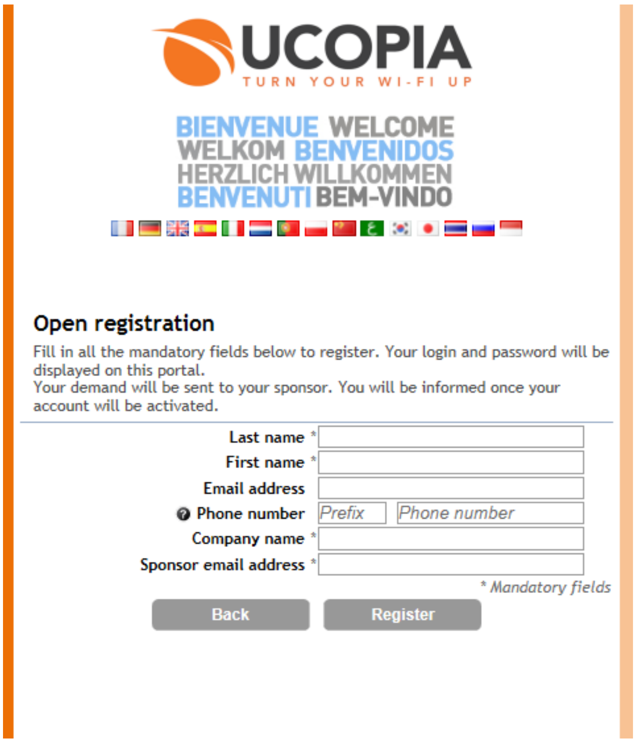
The collected information is stored in the user logs for traceability purposes and/or Marketing. They can in particular be used by Analytics tools (see Section 8.2).

3.3.2 Sponsoring

To enhance the security for self-registering modes, it is possible to validate the registration by a third party, a sponsor.

Thus during the self-registration on the portal, the user enters the email of the sponsor to whom the demand will be sent. The sponsor receives an email with two links allowing to accept or reject the request. The user is notified of the decision on the portal or by SMS.

This sponsoring mode can be activated at portal configuration level. It is available for self-registering modes by email, SMS and form.



Open registration

Fill in all the mandatory fields below to register. Your login and password will be displayed on this portal.
Your demand will be sent to your sponsor. You will be informed once your account will be activated.

Last name *	
First name *	
Email address	
Phone number	Prefix Phone number
Company name *	
Sponsor email address *	

* Mandatory fields

Figure 20: Portal with sponsoring

3.3.3 User account refill

UCOPIA proposes management codes that allow end-users, once entered a code on the captive portal, to refill their account. It is then possible, for example, to get more time credit or bandwidth. These codes can be sold, for example, by an operator through recharge cards sold in different points of sale.

The codes are created through the administration tool, the association of a refill option to a code can be performed either from the administration tool or from the delegation portal.

The refill user account can also be done by online payment without code. Payment can be performed using either PayPal or Ingenico solutions.

3.3.4 Delegation portal

The system administration manager provides full control over the UCOPIA controllers but it is used by MIS staff only. However, many day-to-day operations such as creating, updating or deleting a guest account. With UCOPIA, the IT manager can delegate identified users access the management of guest accounts. Using the delegation administration portal is a 4 steps process and does not require any IT expertise:

Delegate administrators can be defined locally in the UCOPIA directory or belong to an external corporate directory (Active Directory, for instance).

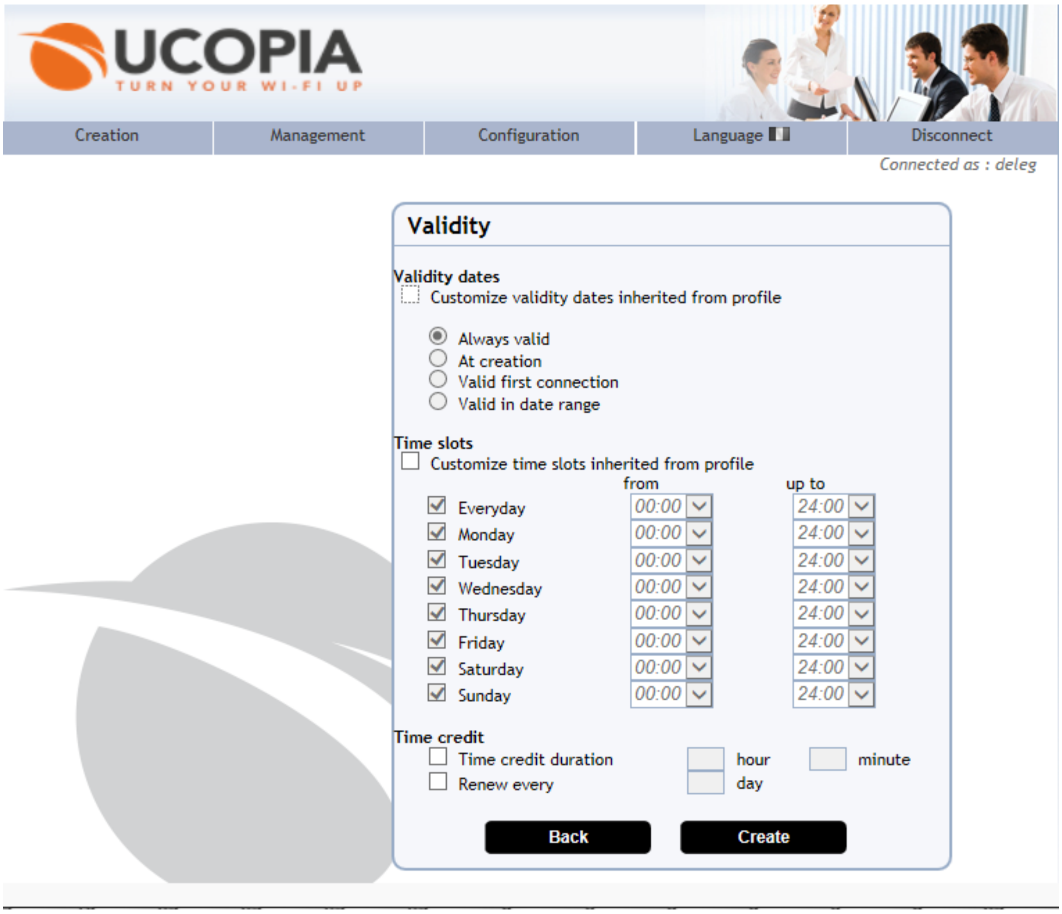
3.3.4.1 Delegate administrator permissions

The UCOPIA administrator is able to adapt the delegation portal on the basis of usage and users. The administrator can consequently set up different profiles with more or fewer permissions. The delegation portal will then be automatically adapted to match the user's permissions. For instance, in the simplest case, the tool may be reduced to its most basic level, generating a connection ticket based just on the user's last name and first name. For more complex tasks, the delegate administrator can be authorized to create an account by allocating a profile and a time slot. Delegate administrators may be able to change the account after creation, re-print a connection ticket, generate a new password, delete an account, etc.

Here is an example of using the delegation portal.

1. Select the guest profile among several guest profiles defined by IT staff
2. Collect the guest information (name, company)
3. Choose time frame and/or time credit
4. Generate a connection ticket summarizing the data the user needs in order to connect (login, password, time restrictions, etc.)
5. The ticket may be printed or sent by email or SMS, depending on the UCOPIA options set up.

The screenshots below show how to select connection time slots and/or time credit from the delegation portal.



Connected as : deleg

Validity

Validity dates

☐ Customize validity dates inherited from profile

● Always valid
○ At creation
○ Valid first connection
○ Valid in date range

Time slots

☐ Customize time slots inherited from profile

	from	up to
☑ Everyday	00:00	24:00
☑ Monday	00:00	24:00
☑ Tuesday	00:00	24:00
☑ Wednesday	00:00	24:00
☑ Thursday	00:00	24:00
☑ Friday	00:00	24:00
☑ Saturday	00:00	24:00
☑ Sunday	00:00	24:00

Time credit

☐ Time credit duration hour minute
☐ Renew every day

Figure 21: Delegation portal – Time slots

3.3.4.2 Customization of the delegation portal

The delegation portal is customizable in "Edit" mode, which can be used to change the wallpaper, logo, add images, text, etc.

3.3.4.3 Multi zones

In the same way as the authentication portal, the delegation portal can have different versions. For example, under a centralized architecture, a hotel chain could offer each of its brands a delegation portal in that brand's colour scheme.

3.3.4.4 Generating multiple accounts

The delegation portal also allows launching large numbers of guest accounts in one batch (for instance from a CSV spreadsheet). This is well suited to host a seminar or a conference. Connection tickets can be printed or sent by email or text message.

3.3.4.5 User accounts refill

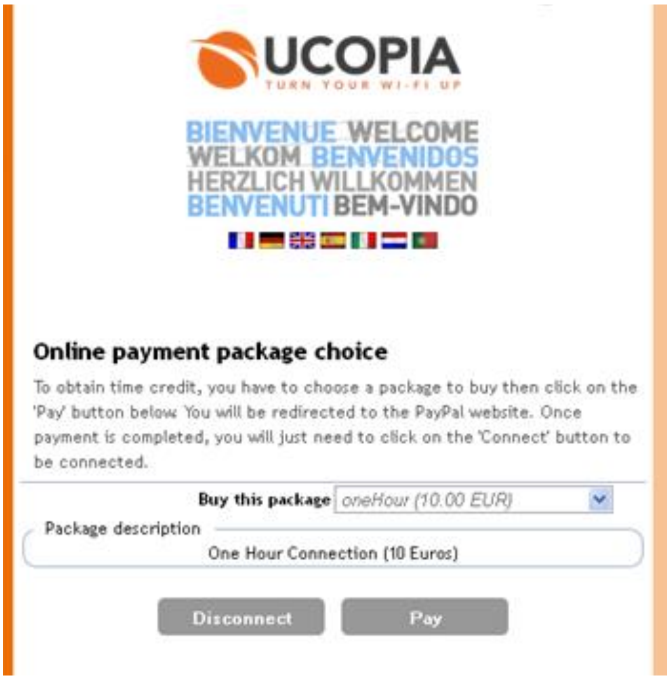
The delegation portal can refill a user account from refill options (e.g. time credit). It also offers the ability to in mass creation of refill codes.

3.4 Billing

UCOPIA lets you implement payment solutions, online payment from the captive portal, or interface with third party billing tools.

3.4.1 On-line payment

Users can purchase connection time or time credit by making an on-line payment. Users are asked to select a package on the UCOPIA portal and are then redirected to the PayPal or Ingenico site, where payment can be made either using a PayPal account or with a credit card (PayPal, Ingenico). Once the transaction is successfully completed, the user can connect to the UCOPIA portal with the login and password delivered by UCOPIA on the portal. Logins and passwords can optionally be delivered via SMS. Traceability is provided because UCOPIA retrieves users' personal details from the payment site. To implement this kind of portal, the organization using UCOPIA has to have a PayPal or Ingenico account in order to receive the money for user purchases.



Online payment package choice

To obtain time credit, you have to choose a package to buy then click on the 'Pay' button below. You will be redirected to the PayPal website. Once payment is completed, you will just need to click on the 'Connect' button to be connected.

Buy this package: oneHour (10.00 EUR)

Package description: One Hour Connection (10 Euros)

Figure 22: Portal with online payment and payment options

3.4.2 Use of a PMS (Property Management System)

This portal works in conjunction with a billing product. The UCOPIA/PMS pairing works with the concept of packages. The package is defined by the UCOPIA administrator. This may be a 1 hour or 3 hour package, or an email package, or “All business days from 4 p.m. to 6 p.m.”, etc. Packages are offered for user selection on the UCOPIA portal after authentication.

3.4.3 Use of prepaid cards (PPS)

This portal works in conjunction with a prepaid card product. Each card has a given connection time. Users authenticate themselves on the portal with the username on the card and a captcha code. The time granted by the card and the time used are displayed on the portal after authentication.

3.4.4 Event Management

To meet the needs of environments such as exhibition centers, UCOPIA offers event management. An event is materialized by a package name and a date of validity, e.g. "The auto show of April 4 to 12." An exhibitor may purchase on the captive portal (via Ingenico) an extension of his package for multiple simultaneous connections, for example to provide Internet access to his visitors or employees. A volume discount can be applied to the purchase of additional connections. A summary of payments (as a PDF) may be obtained by the exhibitor from the captive portal.

3.5 Administration

The administration tool is specifically designed for the network administrator. With it, you can manage the mobility policies of the company, the entire configuration of the UCOPIA system, as well as various monitoring and logging aspects.

Administrators may delegate limited administration rights, notably the creation of user accounts, to authorized individuals who are not network specialists. The delegate is given access to a "delegation" portal in order to create or modify user accounts (see Section 3.3.2).

The administration tool and the delegation portal are accessible through a secure HTTPS Web interface.

3.5.1 Administration profiles

Different administration profiles can be created to provide more or less rights to the administrators. For example, an administrator shall be entitled to make changes to network configuration while another can only modify user profiles and authentication portals.

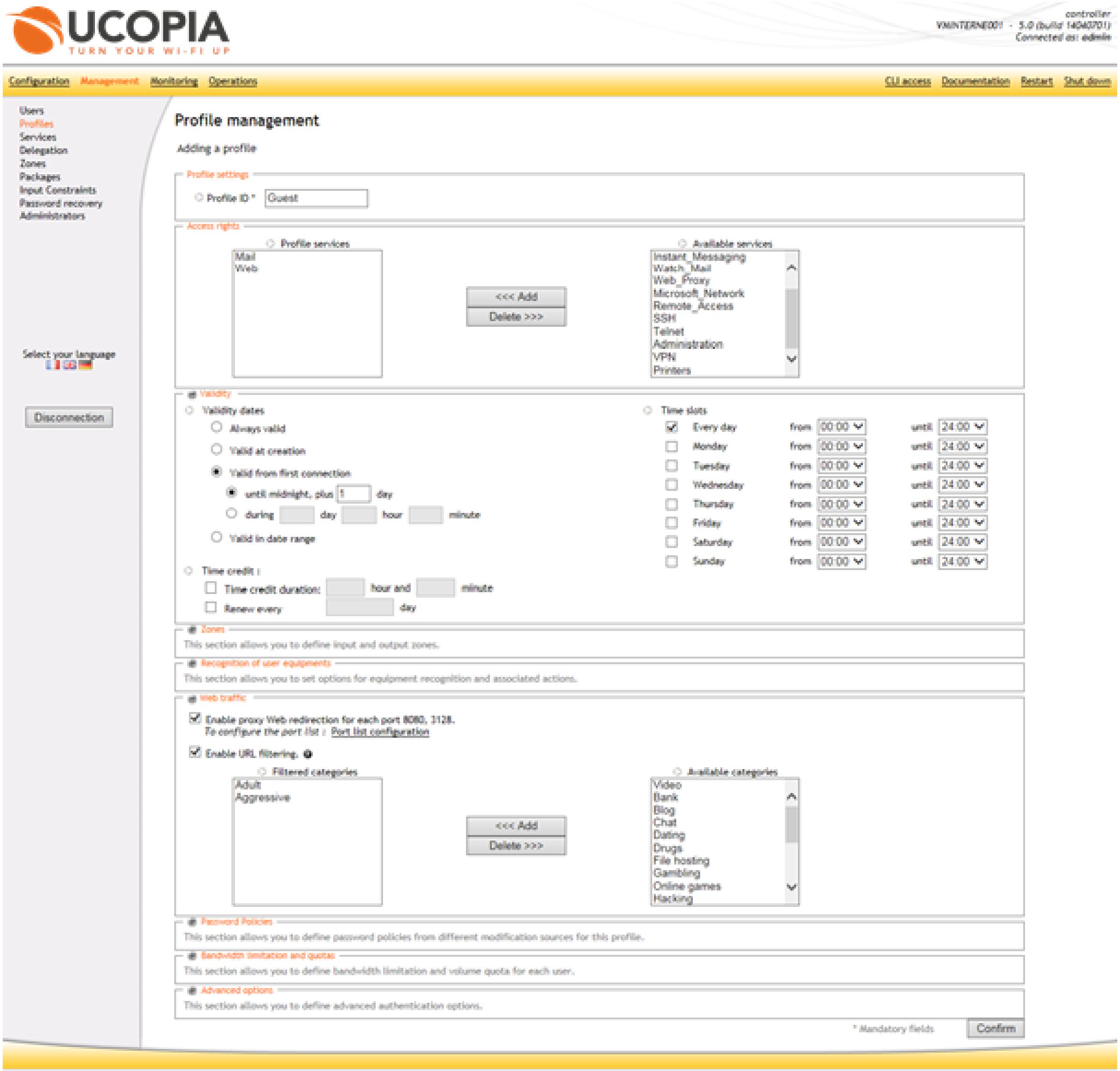
3.5.2 The UCOPIA Mobility Policy administration

The administration tool enables network and security staff to define corporate policies regarding nomadic access (users, applications, zones, time, conditions, QoS, URLs filtering, etc.). With the administration tool, users and groups, services and applications, access rights and credentials, related quality of service can be created, updated and consulted, taking into account time and location. A user inherits from all the services defined in the applicable profile(s) but some rights can be refined at user level.

Services are characterized by IP address, port, and network protocol so that the UCOPIA filtering engine can identify each of them. UCOPIA has a set of predefined services including Internet, mail, various VPN, FTP, URL, etc. Existing services can be modified or removed and new services can be added.

The URLs categories to be banned can be specified at user profile level.

The screenshot below shows the user profile creation with definition of access rights, time slots and authorized URLs.



Profile management

Adding a profile

Profile settings

Profile ID * Guest

Access rights

Profile services	Available services
Mail Web	Instant_Messaging Watch_Mail Web_Proxy Microsoft_Network Remote_Access SSH Telnet Administration VPN Printers

Validity

Validity dates

○ Always valid
○ Valid at creation
● Valid from first connection
● until midnight, plus 1 day
○ during day hour minute
○ Valid in date range

Time credit :

□ Time credit duration: hour and minute
□ Renew every day

Time slots

☑	Every day	from	00:00	until	24:00
□	Monday	from	00:00	until	24:00
□	Tuesday	from	00:00	until	24:00
□	Wednesday	from	00:00	until	24:00
□	Thursday	from	00:00	until	24:00
□	Friday	from	00:00	until	24:00
□	Saturday	from	00:00	until	24:00
□	Sunday	from	00:00	until	24:00

Zones

This section allows you to define input and output zones.

Recognition of user equipments

This section allows you to set options for equipment recognition and associated actions.

Web traffic

☑ Enable proxy Web redirection for each port 8080, 3128.
To configure the port list : Port list configuration

☑ Enable URL filtering.

Filtered categories	Available categories
Adult Aggressive	Video Bank Blog Chat Dating Drugs File hosting Gambling Online games Hacking

Password Policies

This section allows you to define password policies from different modification sources for this profile.

Bandwidth limitation and quotas

This section allows you to define bandwidth limitation and volume quota for each user.

Advanced options

This section allows you to define advanced authentication options.

* Mandatory fields

Figure 23: User profile Definition

3.5.3 Supervision and traceability

UCOPIA manages session and traffic logs, these logs being created locally on the UCOPIA box and available from the UCOPIA administration tool.

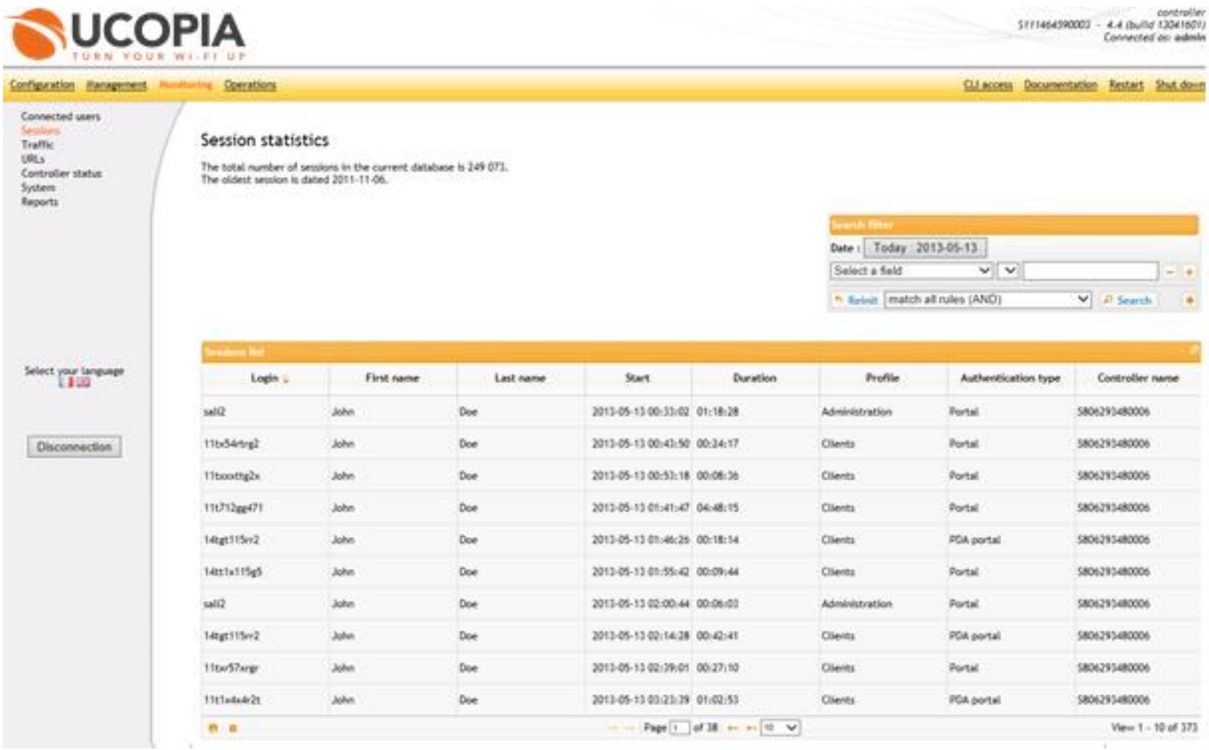
- Session logs

  The sessions log contains the following information:

  - **User login**
  - **Equipment information: IP and MAC addresses**
  - **Incoming subnetworks where the user is connected**
  - **Authentication mode: Web portal, 802.1x, mobile**
  - **Time information: Connection and disconnection time**
  - **User profile**

- **User's Personal information coming from captive portal or social networks: first name, last name, email, phone number, birthdate, gender, interests, etc.**
- **Additional fields added by the administrator, such as company name or i/d card number.**

The screenshot below shows the log view available with UCOPIA.



Session statistics

The total number of sessions in the current database is 249 073.
The oldest session is dated 2011-11-06.

Login	First name	Last name	Start	Duration	Profile	Authentication type	Controller name
sali2	John	Doe	2013-05-13 00:33:02	01:18:28	Administration	Portal	S806293480006
11tx54rtrg2	John	Doe	2013-05-13 00:43:50	00:24:17	Clients	Portal	S806293480006
11txxxttg2x	John	Doe	2013-05-13 00:53:18	00:08:36	Clients	Portal	S806293480006
11t712gg471	John	Doe	2013-05-13 01:41:47	04:48:15	Clients	Portal	S806293480006
14tgt115rr2	John	Doe	2013-05-13 01:46:26	00:18:14	Clients	PDA portal	S806293480006
14tt1x115g5	John	Doe	2013-05-13 01:55:42	00:09:44	Clients	Portal	S806293480006
sali2	John	Doe	2013-05-13 02:00:44	00:06:03	Administration	Portal	S806293480006
14tgt115rr2	John	Doe	2013-05-13 02:14:28	00:42:41	Clients	PDA portal	S806293480006
11txr57xrgr	John	Doe	2013-05-13 02:29:01	00:27:10	Clients	Portal	S806293480006
11t1x4x4r2t	John	Doe	2013-05-13 03:23:39	01:02:53	Clients	PDA portal	S806293480006

Figure 24: UCOPIA sessions log

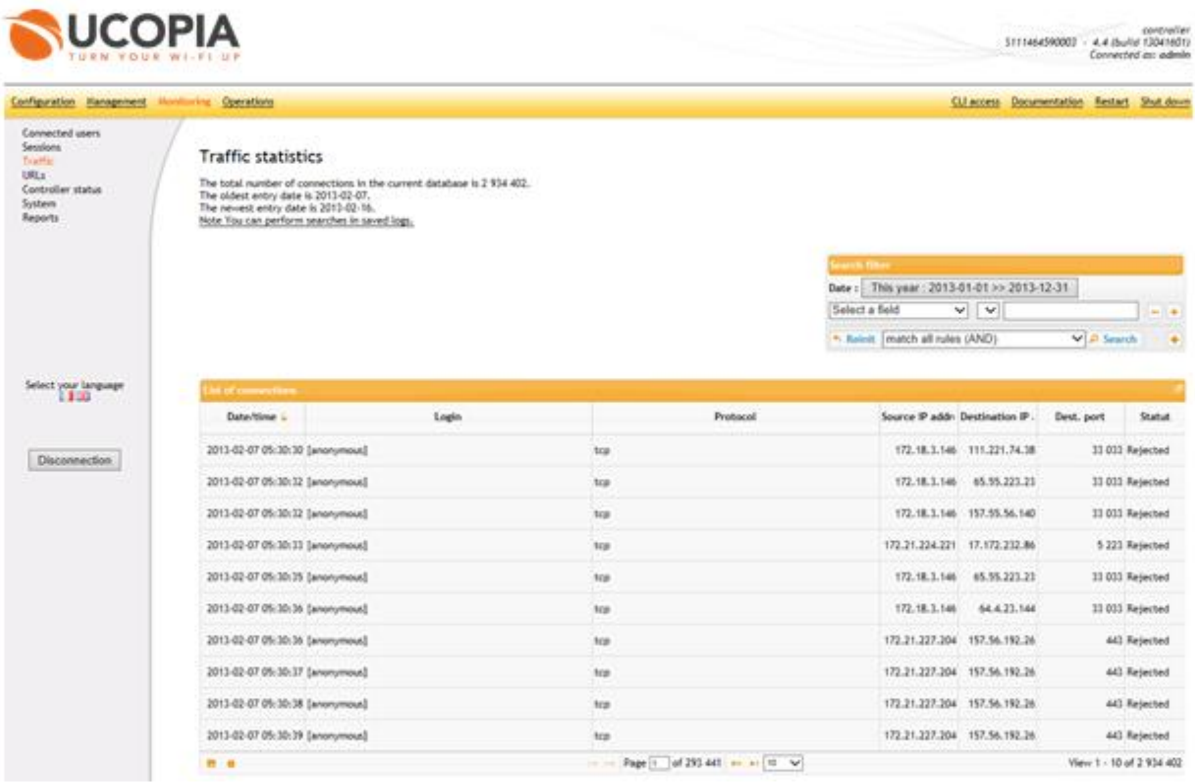
- Activity or traffic logs

The traffic log contains the following information:

- **The services used, and the usage frequency**
- **The source and destination IP addresses**
- **The ports numbers**
- **The URLs**

The screenshot below shows the log view available with UCOPIA.

-



Traffic statistics

The total number of connections in the current database is 2 934 402.
The oldest entry date is 2013-02-07.
The newest entry date is 2013-02-16.
Note You can perform searches in saved logs.

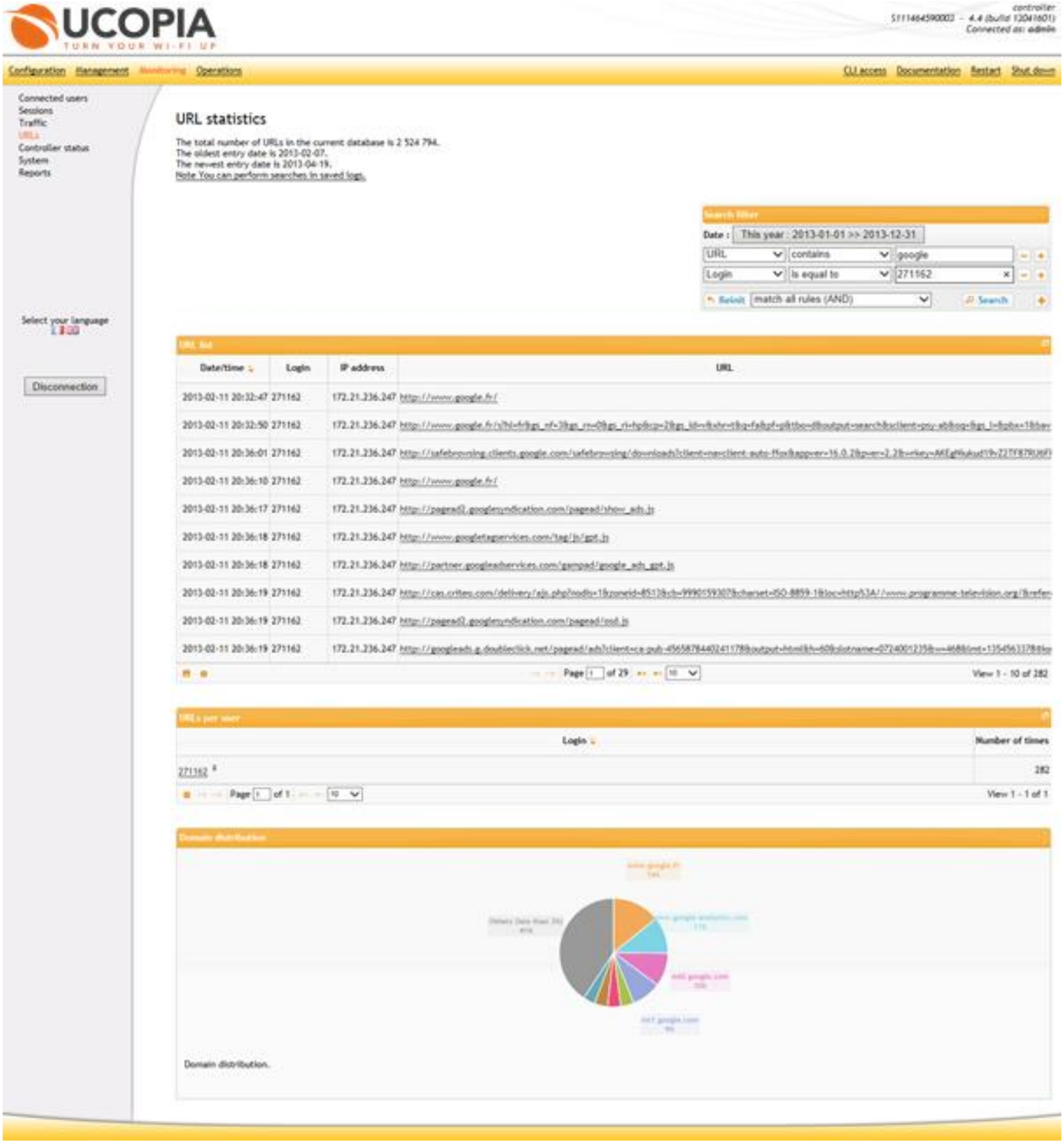
Date : This year : 2013-01-01 >> 2013-12-31
match all rules (AND)

Date/time	Login	Protocol	Source IP addr.	Destination IP .	Dest. port	Statut
2013-02-07 05:30:30	[anonymous]	tcp	172.18.3.146	111.221.74.38	33 033	Rejected
2013-02-07 05:30:32	[anonymous]	tcp	172.18.3.146	65.55.223.21	33 033	Rejected
2013-02-07 05:30:32	[anonymous]	tcp	172.18.3.146	157.55.56.140	33 033	Rejected
2013-02-07 05:30:33	[anonymous]	tcp	172.21.224.221	17.172.232.86	5 223	Rejected
2013-02-07 05:30:35	[anonymous]	tcp	172.18.3.146	65.55.223.23	33 033	Rejected
2013-02-07 05:30:36	[anonymous]	tcp	172.18.3.146	64.4.23.144	33 033	Rejected
2013-02-07 05:30:36	[anonymous]	tcp	172.21.227.204	157.56.192.26	443	Rejected
2013-02-07 05:30:37	[anonymous]	tcp	172.21.227.204	157.56.192.26	443	Rejected
2013-02-07 05:30:38	[anonymous]	tcp	172.21.227.204	157.56.192.26	443	Rejected
2013-02-07 05:30:39	[anonymous]	tcp	172.21.227.204	157.56.192.26	443	Rejected

Page 1 of 293 441 | 10 | View 1 - 10 of 2 934 402

Figure 25: Per user traffic log

Searching for a user on the basis of one item of data is especially straightforward. For example, the screen shot below shows the result of a search for users "who have visited the URL www.google.com within a given period of time". UCOPIA finds the user(s) meeting the criterion. All pages visited are shown.



controller
5111464590003 – 4.4 (build 13041601)
Connected as: admin

Configuration Management Monitoring Operations — CLI access Documentation Restart Shut down

Connected users
Sessions
Traffic
URLs
Controller status
System
Reports

Select your language

Disconnection

URL statistics

The total number of URLs in the current database is 2 524 794.
The oldest entry date is 2013-02-07.
The newest entry date is 2013-04-19.
Note You can perform searches in saved logs.

Search filter

Date : This year : 2013-01-01 >> 2013-12-31
URL | contains | google
Login | is equal to | 271162
Reinit | match all rules (AND) | Search

URL list

Date/time	Login	IP address	URL
2013-02-11 20:32:47	271162	172.21.236.247	http://www.google.fr/
2013-02-11 20:32:50	271162	172.21.236.247	http://www.google.fr/s?hl=fr&gs_nf=3&gs_rn=0&gs_ri=hp&cp=2&gs_id=f&xhr=t&q=fa&pf=p&tbo=d&output=search&client=psy-ab&oq=&gs_l=&pbx=1&bav
2013-02-11 20:36:01	271162	172.21.236.247	http://safebrowsing.clients.google.com/safebrowsing/downloads?client=navclient-auto-ffox&appver=16.0.2&pver=2.2&wrkey=AKEgNi[illegible]
2013-02-11 20:36:10	271162	172.21.236.247	http://www.google.fr/
2013-02-11 20:36:17	271162	172.21.236.247	http://pagead2.googlesyndication.com/pagead/show_ads.js
2013-02-11 20:36:18	271162	172.21.236.247	http://www.googletagservices.com/tag/js/gpt.js
2013-02-11 20:36:18	271162	172.21.236.247	http://partner.googleadservices.com/gampad/google_ads_gpt.js
2013-02-11 20:36:19	271162	172.21.236.247	http://cas.criteo.com/delivery/ajs.php?nodis=1&zoneid=8513&cb=99901593078charset=ISO-8859-1&loc=http%3A//www.programme-television.org/&refer
2013-02-11 20:36:19	271162	172.21.236.247	http://pagead2.googlesyndication.com/pagead/osd.js
2013-02-11 20:36:19	271162	172.21.236.247	http://googleads.g.doubleclick.net/pagead/ads?client=ca-pub-4565878440241178&output=html&h=60&slotname=0724001235&w=468&lmt=1354563178&lo

Page 1 of 29 — 10 — View 1 - 10 of 282

URLs per user

Login	Number of times
271162	282

Page 1 of 1 — 10 — View 1 - 1 of 1

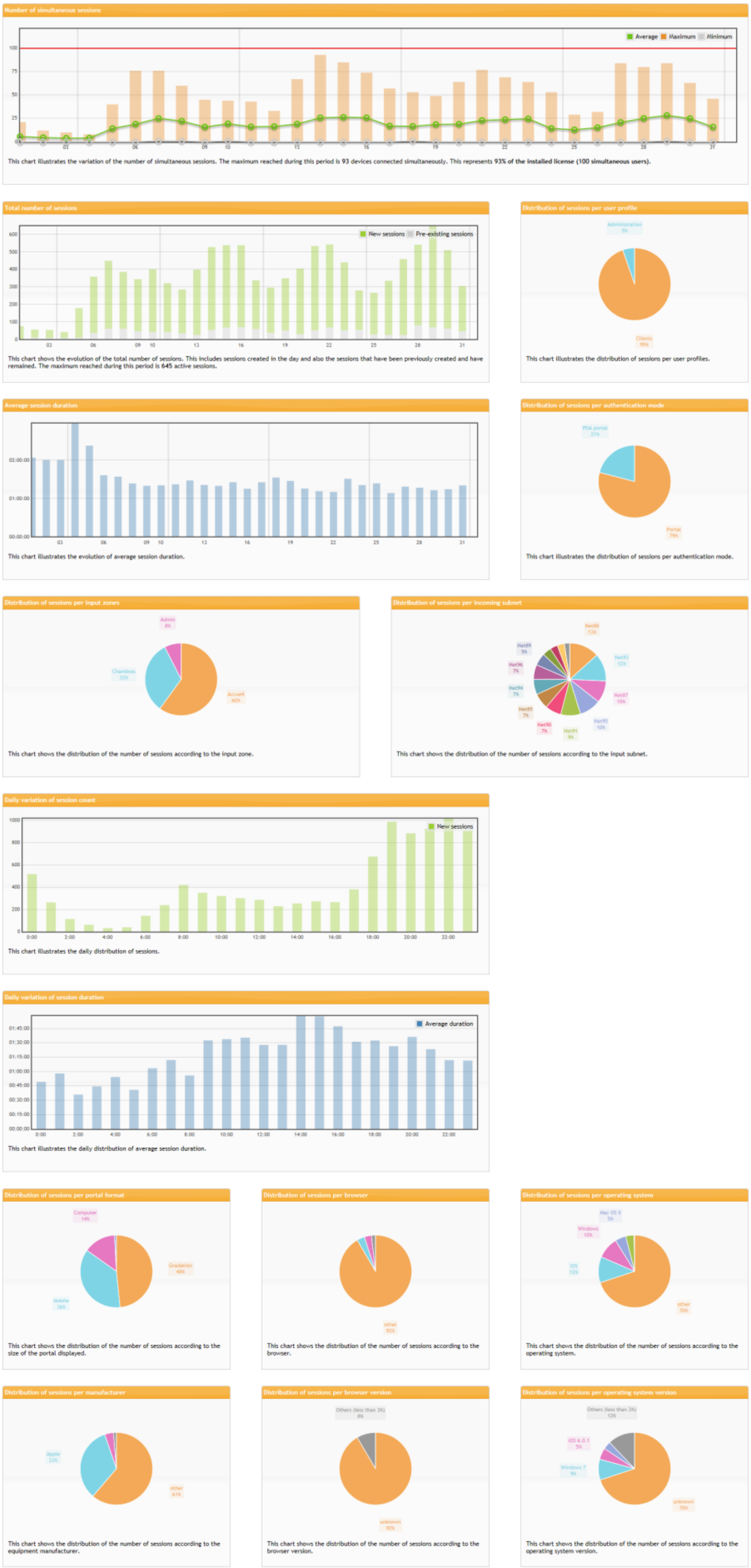
Domain distribution

Domain distribution.

Figure 26: Traffic logs (URLs visited by a named user)

Logs are dynamically compressed to maximize space on the UCOPIA controller. The logs can also be exported manually or automatically (via FTPS) to a third machine.

Logs can also be used for statistical purposes, especially for improved knowledge about the use made of the UCOPIA box. To do so, UCOPIA offers various preconfigured statistical views.



Number of simultaneous sessions

This chart illustrates the variation of the number of simultaneous sessions. The maximum reached during this period is 93 devices connected simultaneously. This represents **93% of the installed license (100 simultaneous users).**

Total number of sessions

This chart shows the evolution of the total number of sessions. This includes sessions created in the day and also the sessions that have been previously created and have remained. The maximum reached during this period is **645** active sessions.

Distribution of sessions per user profile

This chart illustrates the distribution of sessions per user profiles.

Average session duration

This chart illustrates the evolution of average session duration.

Distribution of sessions per authentication mode

This chart illustrates the distribution of sessions per authentication mode.

Distribution of sessions per input zones

This chart shows the distribution of the number of sessions according to the input zone.

Distribution of sessions per incoming subnet

This chart shows the distribution of the number of sessions according to the input subnet.

Daily variation of session count

This chart illustrates the daily distribution of sessions.

Daily variation of session duration

This chart illustrates the daily distribution of average session duration.

Distribution of sessions per portal format

This chart shows the distribution of the number of sessions according to the size of the portal displayed.

Distribution of sessions per browser

This chart shows the distribution of the number of sessions according to the browser.

Distribution of sessions per operating system

This chart shows the distribution of the number of sessions according to the operating system.

Distribution of sessions per manufacturer

This chart shows the distribution of the number of sessions according to the equipment manufacturer.

Distribution of sessions per browser version

This chart shows the distribution of the number of sessions according to the browser version.

Distribution of sessions per operating system version

This chart shows the distribution of the number of sessions according to the operating system version.

Figure 27: Viewing statistics

Session and traffic knowledge enables IT managers to tune and optimize the networking infrastructure, understand which applications are most frequently users and by which users. To take advantage of this logged information, UCOPIA provides with predefined graphics and charts.

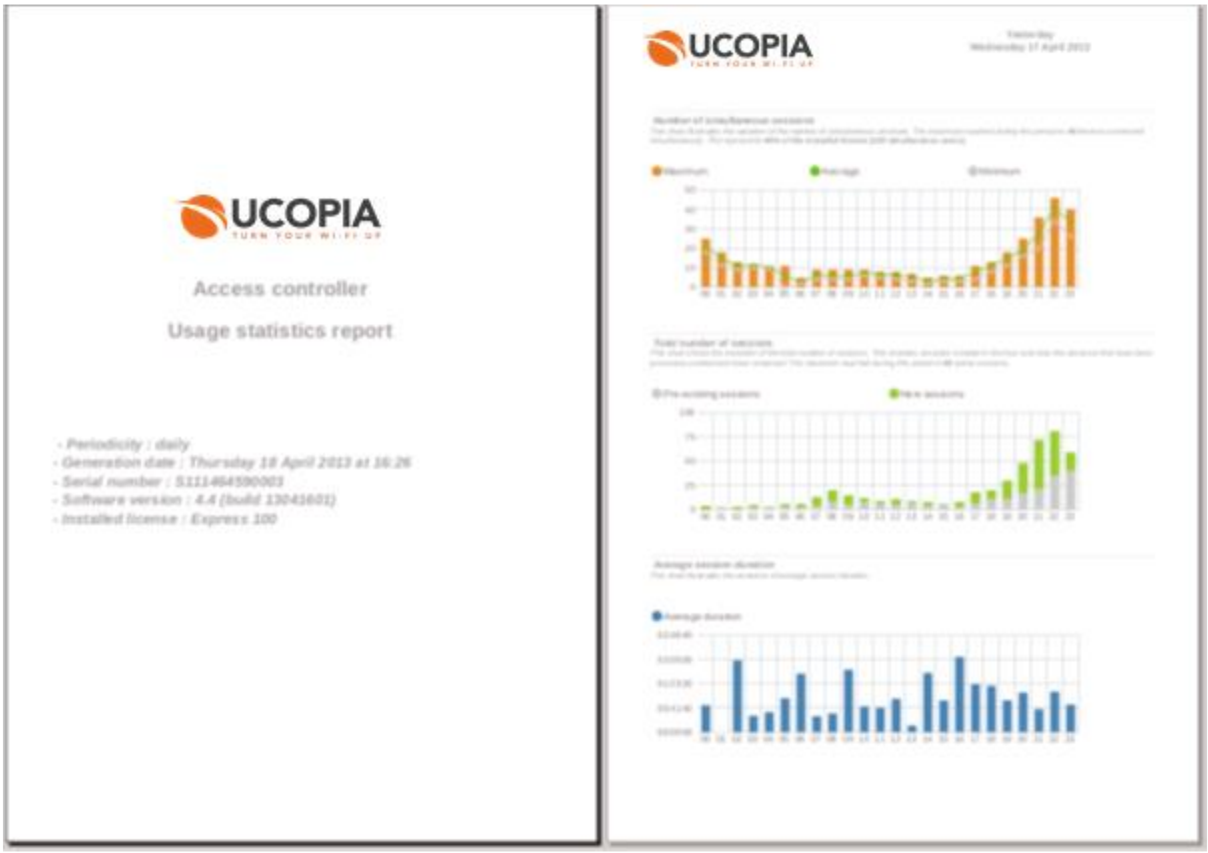
3.5.4 Reporting

A statistical report of user sessions in PDF format can be generated automatically and periodically (daily, weekly, etc.). The report can be emailed to one or more recipients or send to an FTP server.

Reports can be generated per zone.

The report includes statistics such as:

- Number of simultaneous connections
- Total number of sessions
- Average duration of sessions
- Number of sessions per authentication mode, per user profile, …
- Number of sessions per incoming subnet, per zone, …
- Number of session per equipment type, per operating system, …
- Most consumer users in terms of bandwidth
- etc.



Access controller

Usage statistics report

- Periodicity : daily
- Generation date : Thursday 18 April 2013 at 16:26
- Serial number : S111464590003
- Software version : 4.4 (build 13041601)
- Installed license : Express 100

Figure 28: Sample report in PDF format

3.5.5 UCOPIA controller configuration

With the UCOPIA manager, the IT manager can configure the controller: network parameters, VLAN, IP addressing, corporate directories or RADIUS servers integration, etc.

3.5.6 UCOPIA controller administration

Once configured, the controller configuration and data can be archived and restored: directories, logs. The controller firmware can be upgraded locally or remotely through a maintenance tunnel (see Section 0).

3.5.7 Centralized administration

When several controllers are distributed over several locations, UCOPIA enables to define one controller as main controller and others as secondary. The main controller then remotely manages the secondary controllers (see multi controllers architecture section for more details).

3.5.8 SNMP Administration

UCOPIA controllers include an SNMP agent, which means they can be supervised from an SNMP-compatible monitoring tool.

A UCOPIA MIB (Management Information Base) is offered to enable dialogue between the supervision tool and UCOPIA agent. SNMP traps can be triggered to monitor the controller's various active services (DHCP, RADIUS, SQL, etc.).

3.5.9 Administration via CLI

A Command Line Interface (CLI) is available. The aim is to make certain advanced administration tasks possible.

The CLI is available from the administration console. The CLI can be used to view a UCOPIA controller's various internal logs (DHCP, RADIUS, etc.), to run network commands (nslookup, tcpdump, etc.), or to start or view service statuses (DHCP, RADIUS, proxy, LDAP, etc.).

3.5.10 Syslog export

UCOPIA's syslog file, which centralizes the event logs, can be exported from a UCOPIA controller to be loaded onto a syslog server. The events sent can be filtered by category (DHCP, RADIUS, etc.).

3.5.11 Multi sites administration

In the case of a multi sites centralized architecture, it is interesting to dedicate administration operations at each site. For this, on the central controller, an entry zone may be associated with a site. It will then be possible to administrate at the zone level, for example by allocating a license per zone, a captive portal, an Ingenico account, etc. The statistical reports can also be generated per zone, the delegation portal and the associated connection tickets as well.

3.5.12 Account management by the end-user

The administrator can give the user the ability to manage his own user account from the captive portal. The user can thus modify his personal information (name, email, ...) and manage his equipment list. Indeed, in the case where the user's equipments are recorded by the UCOPIA controller, they will be visible from the admin account page. The user then has the option to manage his devices, for example, for removing a device that no longer exists.

4 UCOPIA architecture

In this section, the UCOPIA main components, APIs and protocols are described. The UCOPIA controller fits between the WLAN and the legacy corporate LAN.

The user traffic is forced through the UCOPIA controller, based on physical (cable) or logical (VLAN) configuration. Authentication protocols between the user and the controller can be HTTPS or EAP. The UCOPIA RADIUS and the administration tools connect to the corporate directory through the Secure LDAP (LDAPS). Traceability is supported by an embedded SQL database. Administration relies on an HTTPS secure WEB protocol.

The UCOPIA appliance is built on top of industry hardware components (processor, memory, disk) and a Linux operating system.

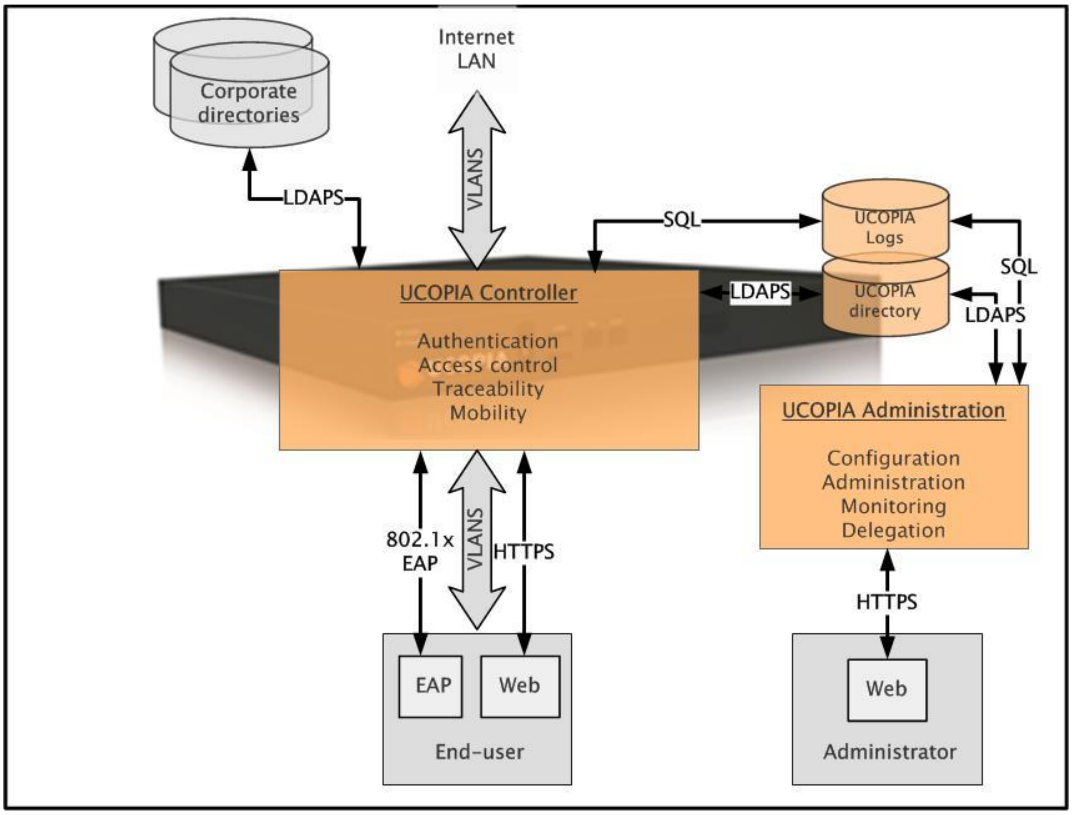


Figure 29: UCOPIA architecture

4.1 UCOPIA Controller

The UCOPIA controller is the corner stone of the UCOPIA architecture. It enforces corporate mobility policies defined with the system administration tools and stored in the directory. The controller includes the RADIUS server, and modules to manage access control, quality of service, URLs filtering, zero configuration, etc. The **Security and Mobility Manager** controls all these modules.

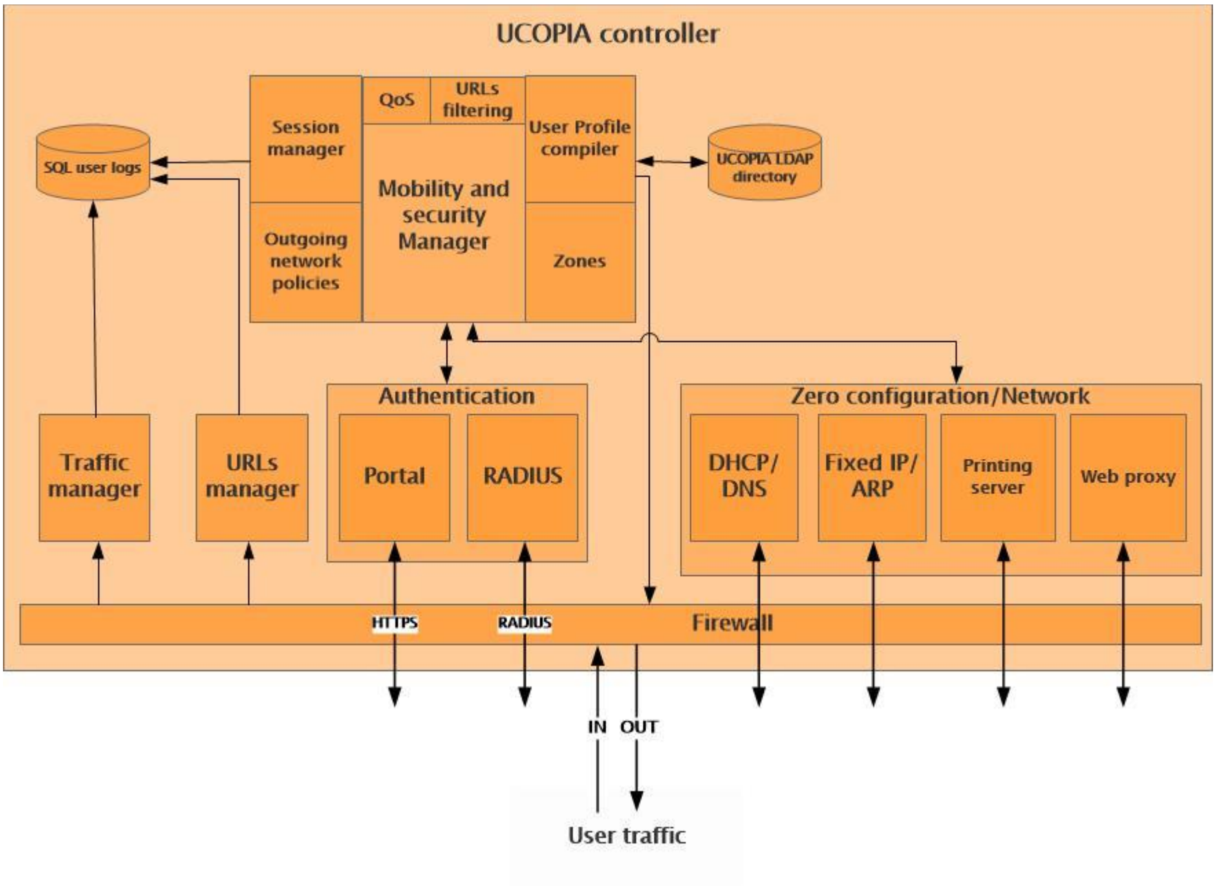


Figure 30: The UCOPIA Controller architecture

The controller stands on top of a filtering engine used to classify, control, redirect log sessions and traffic. The filtering engine uses IP and MAC addresses, port numbers, protocols, etc. The UCOPIA filtering engine stands on top of Linux components such as IP Tables, Netfilters and more.

- **Authentication:** The controller embeds a RADIUS server which serves as the authentication server for the 802.1x protocol. The RADIUS server supports various authentication algorithms including TLS, TTLS, PEAP, etc. The RADIUS can query a corporate directory (LDAP V2 or V3, Active Directory) or a cascade of directories (for instance first employee directory then partners and customers). The UCOPIA portal implements WEB HTTPS based login/password authentication. This authentication method can also be used via RADIUS, a solution which is useful for architectures based on connecting RADIUS servers with a proxy mechanism. UCOPIA can query UCOPIA's LDAP directory and/or one or more external directories to carry out authentication.
- **Access control**: At authentication time, the Access control module in the controller gets the user profile from the directory. This profile is made of high level mobility policies which are dynamically compiled into low level filtering rules in the controller. These rules are automatically and dynamically activated removed when the user disconnects.
- **Quality of service:** The UCOPIA controller identifies the up going and ingoing traffic and marks the packets according to predefined policies (normal and high priorities, guaranteed or maximum bandwidth) depending on profile and applications. Traffic classification and priority management is implemented in the UCOPIA QoS module. Packets are dispatched into queues in order to implement priority management.
- **URLs filtering :** The « URLs filtering » module allows to filter URLs coming from the user traffic. Only authorised URLs will be accessed. Filtering works with predefined categories, the URLs database is embedded into the controller.

- **Seamless access:** The “Zero configuration” module is based on the UCOPIA filter. This module detects misconfigured traffic and fixes the configuration problems automatically, based on the knowledge of the local environment stored in the UCOPIA directory. To do so, the Zero configuration Module implements smart routing algorithms and redirect traffic to the appropriate servers (for instance redirection of outgoing email to the local SMTP server or redirection of Internet access to the local Internet proxy). The Zero configuration module automatically pushes software modules (e.g. printer drivers) needed to use a specific application or service. A printing server is in charge to deliver printer drivers. Moreover, this module delivers @IP in DHCP mode and allows to support devices configured with fixed @IP.
- **Zones:** The « Zones » module implements logical zones which can represent specific areas or sites. In terms of network, a zone can be a set of VLANs or subnet according to the network layer architecture (layer 2 or 3).
- **VLAN redirection:** The UCOPIA Outgoing network policies module can force user traffic in a wired VLAN based on profile policy. This module complies with 802.1q.
- **IP addressing:** The UCOPIA controller contains a DHCP server, a NAT router and a DNS server in order to implement highly flexible addressing schemes and interoperate with legacy wired network strategies.
- **Traceability:** User logs are generated from three sources and stored into an SQL database: The Session Manager logs user sessions (login, firstname, lastname, @IP, @MAC, etc.), the Traffic Manager logs user traffic (IP packet headers), the URLs Manager logs URLs accessed by users.

4.2 The UCOPIA administration Tools

UCOPIA administration is based on a complete set of tools enabling configuration, controller, users, services and policies administration, real time and statistic supervision.

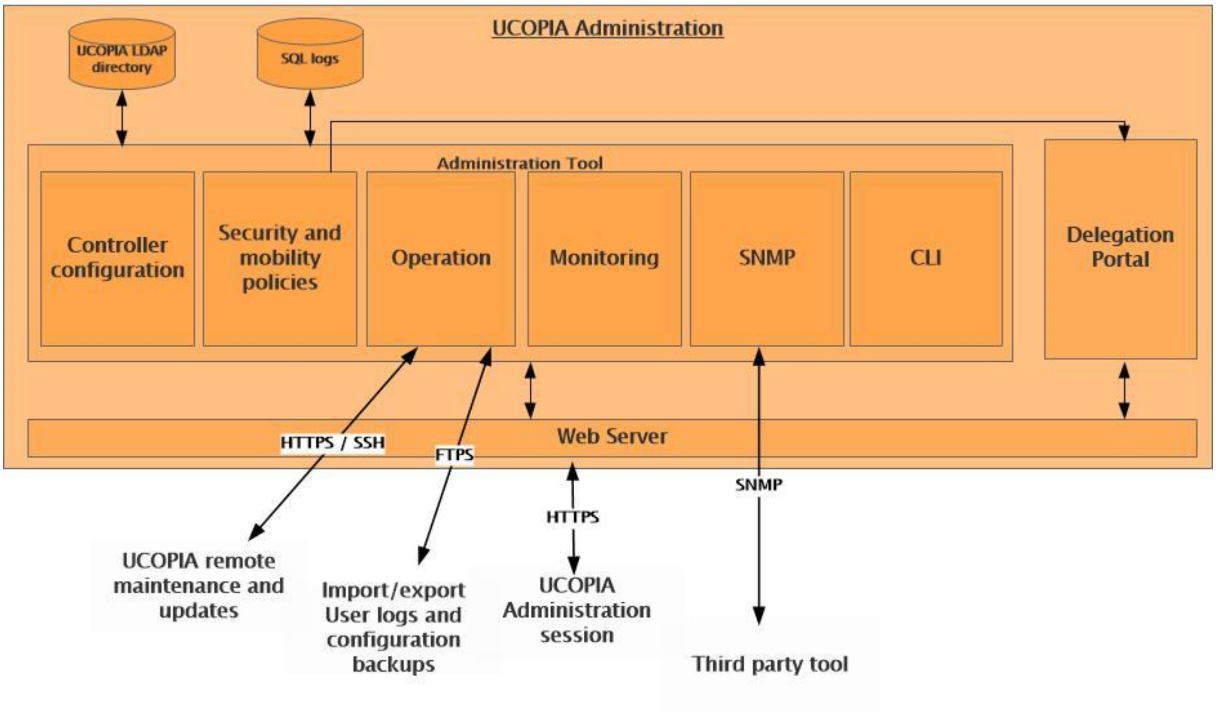


Figure 31: The UCOPIA Administration Manager

- **Configuration: The controller configuration module enables to define network properties (DHCP, DNS, in and out VLANs) as well as the authentication, zero configuration and redundancy/load balancing policies. Customization of the UCOPIA portal and connection tickets is also handled by this module. The configuration can be exported in a file for backup and restore process.**

- **Security and mobility policies: This module enables to create, update, remove the services filtered by UCOPIA, to define profiles (who is allowed to use which services and in which conditions of time, location). This constitutes the UCOPIA mobility model which is stored in an LDAP directory. The secure LDAPS protocol is used to query and update the UCOPIA directory.**
- **Controller(s) supervision and log: UCOPIA controllers can be supervised remotely (who is connected where, for which applications). Connections and sessions logs are stored in an SQL database. The logs can be queried through of the predefined UCOPIA query and more queries can be defined using the SQL query language.**
- **Operation: This module is used to operate the UCOPIA controller: firmware upgrades, configuration backup and restore, remote control and maintenance. Backups and user logs can be manually or automatically imported or exported. Automatic exportation is done via FTPS. Backups are compressed and archived in a .tar format. Releases are downloaded manually from the UCOPIA Extranet web site or automatically from the Services Management Platform.. Remote maintenance relies on an SSH tunnel opened from the controller to the UCOPIA maintenance servers.**
- **SNMP: An SNMP agent means the controller can be supervised from any SNMP-compatible monitoring tool available on the market.**
- **CLI: Command line language for advanced administration.**
- **Delegation portal: The delegation portal enables quick and simple network access provisioning for guests. It is based on a high level graphic WEB interface secured with and HTTPS protocol. This delegation tool uses the UCOPIA directory to store the guest account information.**

4.3 Wi-Fi access points

The prerequisites for Wi-Fi access points depend on the protocols used, in particular during authentication, for example 802.1x authentication will require access points that support this protocol. Access points are configured with several SSIDs, each SSID is encapsulated within a VLAN. A range of IP addresses and an authentication method (802.1x or password) are allocated to each VLAN, which is done so as to isolate the various populations of Wi-Fi users.

The RADIUS server address must be specified in the access points, together with the secret shared with the server.

4.4 User workstation requirements

The requirements for user workstations vary depending on the authentication method.

- **HTTPS Web portal: The user opens a Web browser, and is forced on an authentication Web page hosted in the controller. To do so, UCOPIA uses APACHE to handle the customizable Web portal, SQUID for Web redirection and HTTPS to securely transport the login and password.**
- **802.1x /PEAP or TTLS: With UCOPIA, it is also possible to authenticate with a password through an EAP/802.1x architecture. The benefits are 2 fold: the user authenticates before having an IP address which enhances security and the authentication is mutual (user and infrastructure) so that the user has the guarantee that he/she does not connect on a Rogue. To implement this EAP architecture, UCOPIA relies on a RADIUS server in the controller native user device PEAP (on Windows) or TTLS (Linux, Mac OSX) access point. The certificates used to authenticate the infrastructure can be generated by UCOPIA or third party PKI.**
- **802.1x/EAP-TLS: The authentication key is a certificate. The EAP-TLS authentication protocol is based on a PKI architecture with certificates, which are X509 and installed**

in PKCS#12 (Personal Information Exchange Syntax Standard) format for private key storage. They are installed either directly on the user workstation, or on a smartcard in PKCS#12 format (Public-Key Cryptography Standard). The Windows EAP-TLS environment is available from Windows 2000 Service Pack 3 version onwards. This authentication method requires no client software on the user's workstation.

5 Integrating UCOPIA in legacy LAN infrastructure

UCOPIA is an off the shelf solution integrating all components needed to securely operate a corporate WLAN. These results in the UCOPIA Express controllers product line, best suited for small and medium organizations[4]. UCOPIA also makes it very easy to integrate smoothly with legacy networking and security environments. UCOPIA is based on a highly modular, open architecture so that it can interoperate with existing directories (LDAP, Active Directory, NT Domain, etc.), existing RADIUS, DHCP, VPN servers, VLAN and IP management policies, corporate Intranet and applications authentication and access. All these configuration options are available in the UCOPIA Advance controller product line to match large projects requirements[5].

5.1 Integration with one or several corporate directories

UCOPIA integrates with any corporate directories which comply with the LDAP V3 protocol. In this case, users' accounts are stored in the corporate directories while the UCOPIA directory is used to store the UCOPIA mobility model and the guests accounts. The schema below shows this architecture:

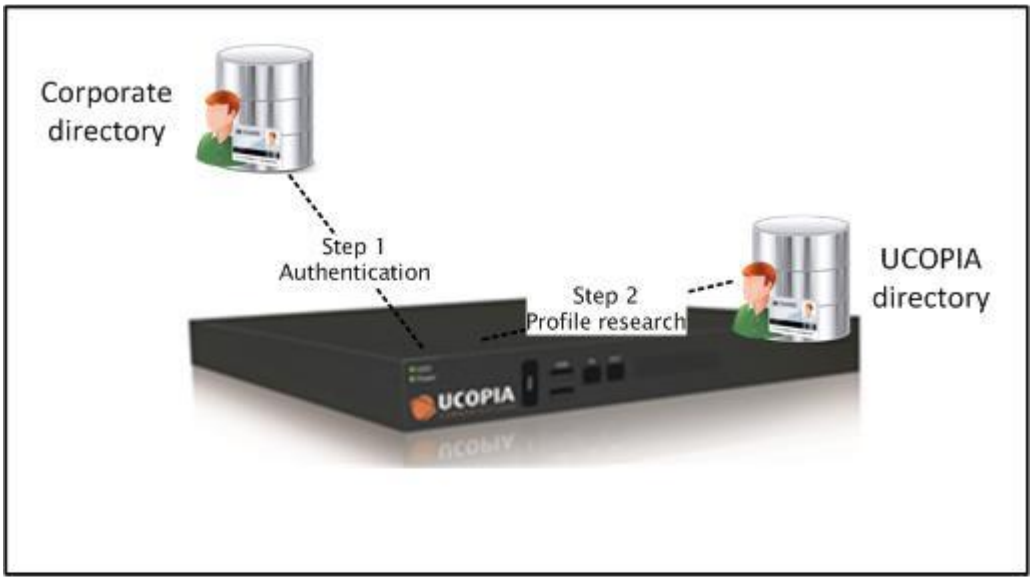


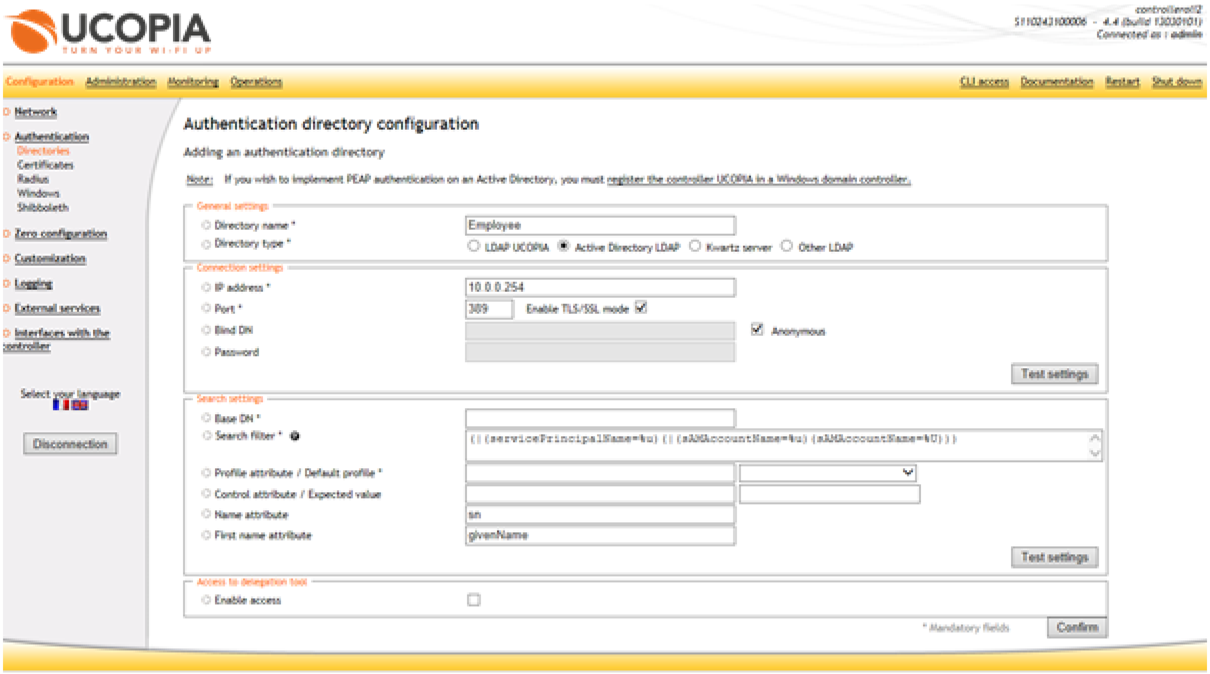
Figure 32: User connection process

To implement this mechanism, it needs to be possible to deduce the profile of a user found in the UCOPIA directory on the basis of data found in the corporate directory.

The following screen shot shows how to configure the connection to an external directory.

[4] UCOPIA Express

[5] UCOPIA Advance



Authentication directory configuration

Adding an authentication directory

Note: If you wish to implement PEAP authentication on an Active Directory, you must register the controller UCOPIA in a Windows domain controller.

General settings

Directory name * Employee

Directory type * ○ LDAP UCOPIA ● Active Directory LDAP ○ Kwartz server ○ Other LDAP

Connection settings

IP address * 10.0.0.254

Port * 389 Enable TLS/SSL mode ☑

Bind DN ☑ Anonymous

Password

Test settings

Search settings

Base DN *

Search filter * (|(servicePrincipalName=%u)(|(sAMAccountName=%u)(sAMAccountName=%U)))

Profile attribute / Default profile *

Control attribute / Expected value

Name attribute sn

First name attribute givenName

Test settings

Access to delegation tool

Enable access □

* Mandatory fields Confirm

Figure 33: Configuring UCOPIA to integrate with the corporate directory

An LDAP filter is used to identify the user; the user profile is obtained in the group attribute.

UCOPIA authentication process can also operate with several corporate directories (local employees, corporate staff, sub-contractors and suppliers, customers, etc.). At authentication time, the user identity is checked by sequentially querying all directories until success. The list of directories is defined and sorted with the UCOPIA administration tool.

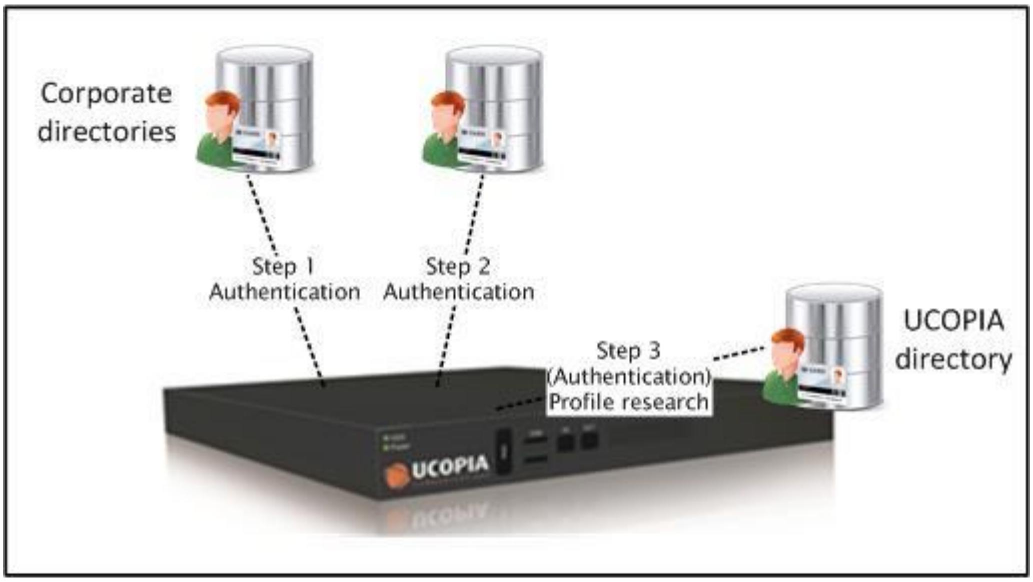
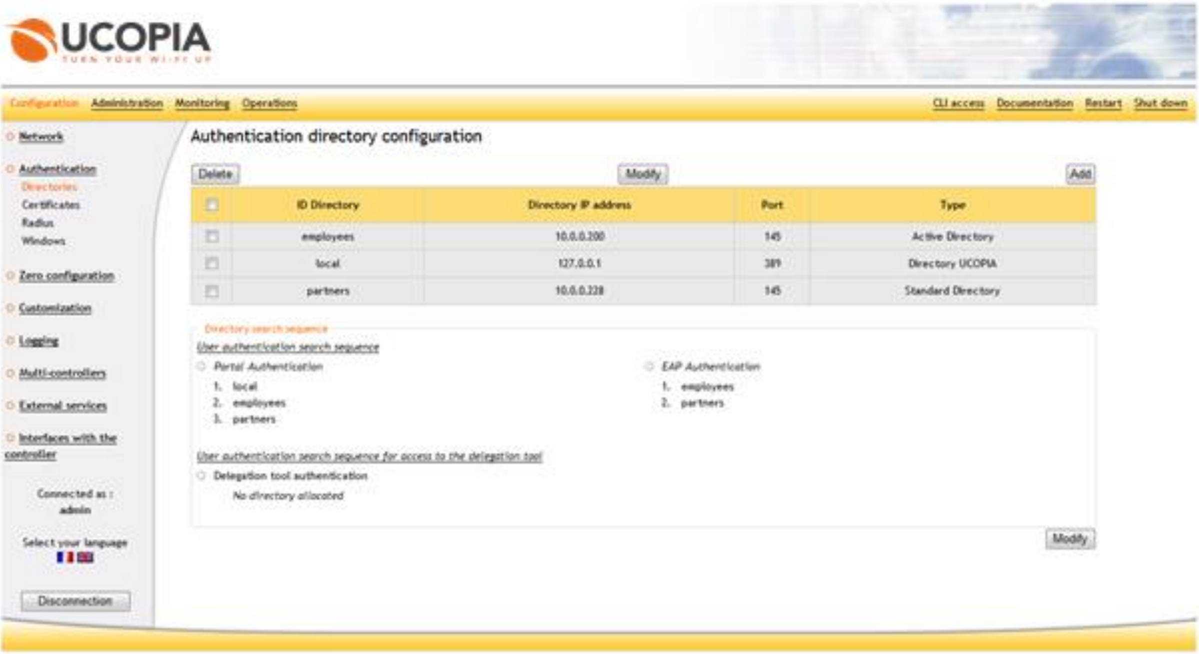


Figure 34: UCOPIA authentication with multiple corporate directories

The screenshot below shows how to configure multiple cascaded directories authentication. In this example, 3 directories are defined (employees, partners and local (ucopia)), and these directories are queried in a different order depending on the authentication mode (web portal, 802.1x).



Authentication directory configuration

□	ID Directory	Directory IP address	Port	Type
□	employees	10.0.0.200	145	Active Directory
□	local	127.0.0.1	389	Directory UCOPIA
□	partners	10.0.0.228	145	Standard Directory

Directory search sequence

User authentication search sequence

○ *Portal Authentication*

1. local
2. employees
3. partners

○ *EAP Authentication*

1. employees
2. partners

User authentication search sequence for access to the delegation tool

○ Delegation tool authentication

No directory allocated

Figure 35: UCOPIA configuration with multiple corporate directories

5.2 IP addressing and VLANs architecture

In the LAN architecture, the UCOPIA controller stands between the access network and the applications network.

Both the access network and the applications network are organized in one or several VLANs each of them owning an IP addressing scheme. UCOPIA enables flexible management of the VLANs and IP address. The UCOPIA controller first includes 2 different Ethernet cards, one to collect the access VLANs, and the second to deal with traffic to and from the applications network VLANs.

UCOPIA embeds a DHCP server and natively operates in NAT mode: By default, one incoming VLAN is configured on a UCOPIA controller (native), usually used for administration purpose. All users exit the UCOPIA box by the same native eth0 interface.

The following diagram shows the default operation of a UCOPIA controller.

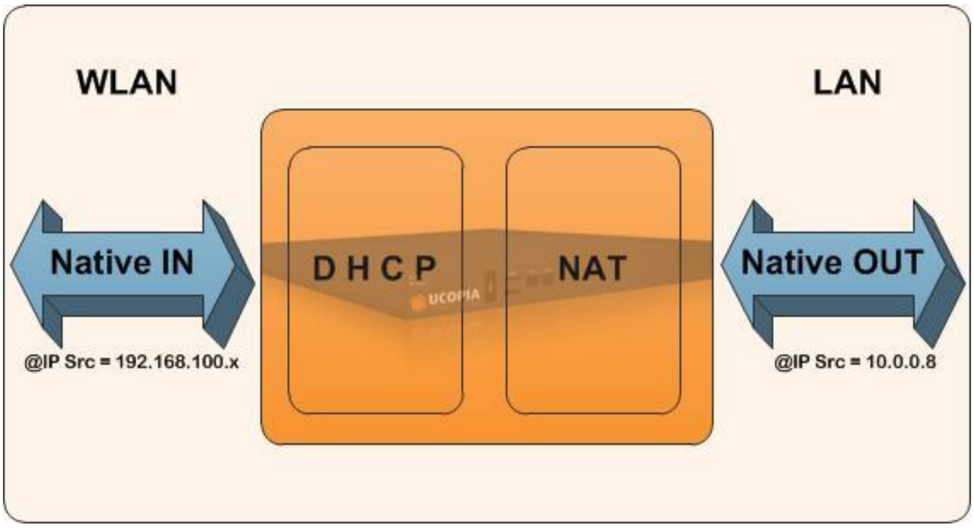


Figure 36: UCOPIA IP & VLAN default configuration

The addressing policy can be customized depending on the user profile. For instance, guests IP address can be translated (NAT mode) while employees are routed. Schema below shows how to configure these 2 addressing policies which impact the traffic going through the UCOPIA controller on the applications network.

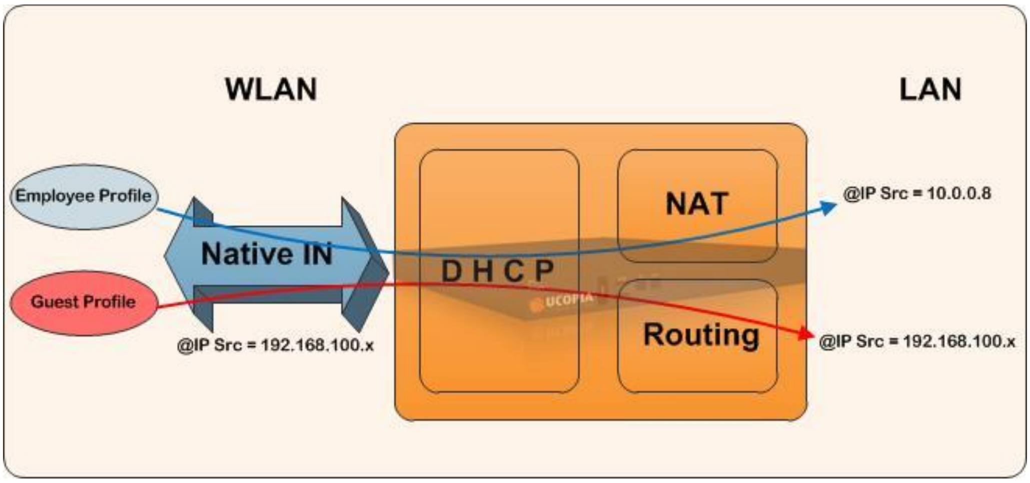


Figure 37: UCOPIA IP management based on user profile

Several outgoing VLANs can be defined with UCOPIA. Depending on user profile, guest traffic can be pushed on a VLAN which forces the user traffic to an Internet router while employee traffic is pushed on a VLAN delivering access to the corporate applications (see below).

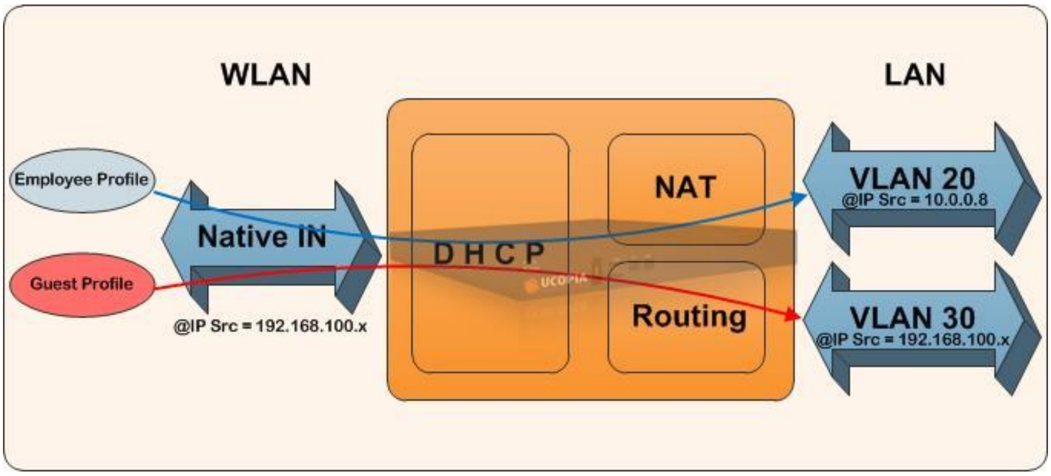


Figure 38: UCOPIA IP and outgoing VLANs management based on user profile

Last, UCOPIA enables the creation of zones (lobby, meeting rooms, etc.). Zones are mapped into one or several VLANs (see Section 6.3).

A user may be authorized to connect in one zone but not in another or get a different profile depending on the connection zone. For instance, an employee connecting in the lobby on the Web portal does not have all the rights he gets in the office space.

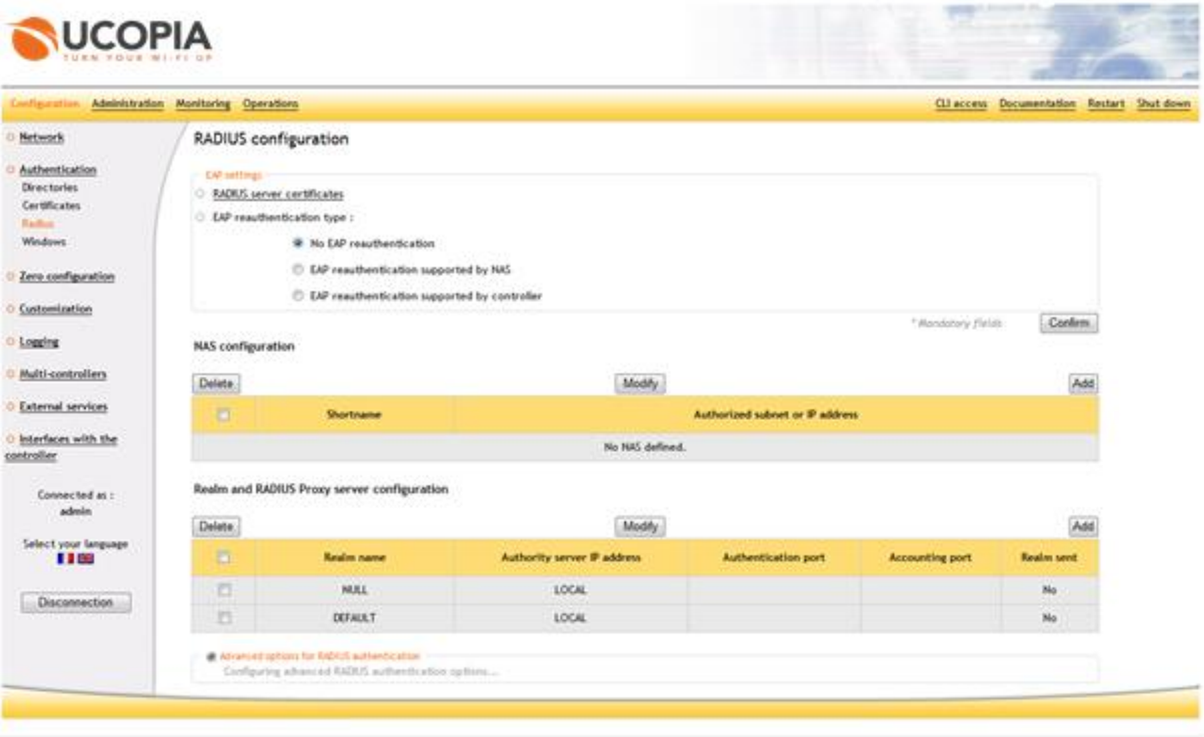
5.3 Integration with a corporate Web proxy

UCOPIA can redirect HTTP traffic to a parent proxy through its own embedded Web proxy. Information specific to the user (*login* and password) can be transmitted to the parent proxy, allowing you to apply different policies to different users.

5.4 Integration with a RADIUS server

The UCOPIA controller has an embedded RADIUS server used for different UCOPIA authentications methods based on 802.1x/EAP. This server can also be used in proxy mode for authentication or accounting requirements.

The screenshot below shows how to configure the UCOPIA RADIUS proxy mode.



RADIUS configuration

EAP settings

○ RADIUS server certificates

○ EAP reauthentication type :

● No EAP reauthentication

○ EAP reauthentication supported by NAS

○ EAP reauthentication supported by controller

* Mandatory fields [Confirm]

NAS configuration

[Delete] [Modify] [Add]

□	Shortname	Authorized subnet or IP address
		No NAS defined.

Realm and RADIUS Proxy server configuration

[Delete] [Modify] [Add]

□	Realm name	Authority server IP address	Authentication port	Accounting port	Realm sent
□	NULL	LOCAL			No
□	DEFAULT	LOCAL			No

● Advanced options for RADIUS authentication

Configuring advanced RADIUS authentication options...

Figure 39: RADIUS configuration

5.5 Integration with a PKI architecture

The UCOPIA solution can take advantage of existing PKI infrastructures.

If the organization has already distributed certificates to its users, then these certificates can be used with UCOPIA to authenticate with UCOPIA.

UCOPIA enables to store in the corporate directory, on the user device and/or in a secure token, with a PKCS12 format. Certificates need an EAP/TLS extension. The UCOPIA controller gets a certificate from the certification authority in order to authenticate itself. The certificate must have a CN attribute which specifies the user identity as defined in the corporate directory.

This attribute is used to query the directory.

5.6 Integration with academic architectures

5.6.1 EDUROAM architecture

The UCOPIA RADIUS server can act as a proxy for another authentication server, or for a particular authentication mode.

This architecture has been deployed in a country wide EDUROAM European student program which we describe now.

EDUROAM is a distributed authentication architecture, based on the RADIUS protocol and providing a global authentication for any student connecting on any campus in the country with a single account and password.

All EDUROAM campus have their own RADIUS server connected to a global EDUROAM proxy. When a student connects on a campus, an authentication query is sent to the EDUROAM proxy, including the user ID in the form of userid@nativecampus.country. This ID is used to forward the authentication query to the RADIUS server “owning” the user.

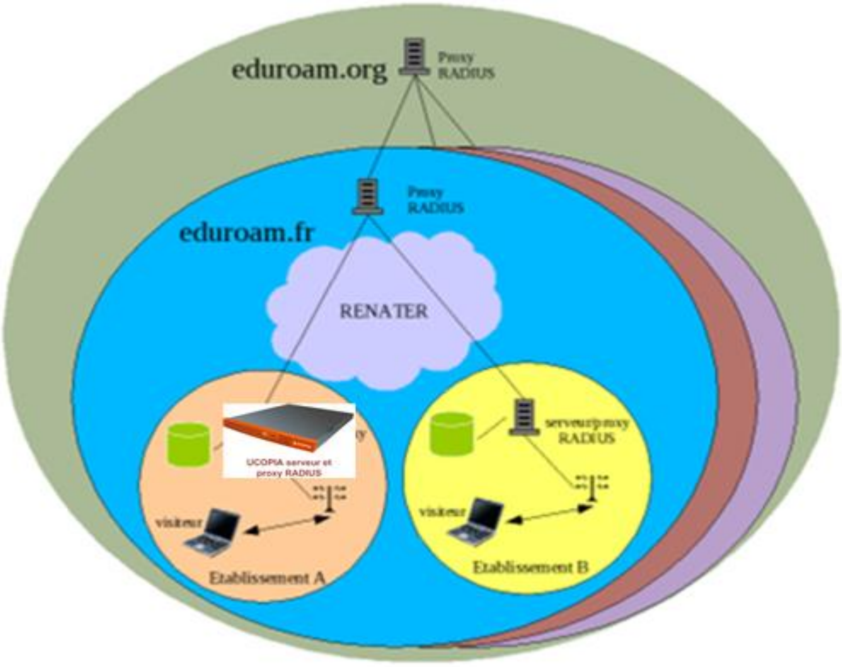


Figure 40: EDUROAM Architecture

UCOPIA fits into this architecture based on the following features:

1. RADIUS proxy
2. The user’s domain is analyzed using the domain (or realm) name associated with the user’s login (being of the user@place.fr type). This enables routing towards the site to which the user belongs.
3. 802.1x/RADIUS authentication or by Web portal paired with RADIUS. In fact, the RADIUS method is conventionally the authentication server under 802.1x architecture. UCOPIA combines the ease of use of the Web portal method with the RADIUS method and RADIUS proxy.

5.6.2 Shibboleth architecture

The Shibboleth software is developed by the Internet2 Middleware Initiative. Shibboleth implements widely used federated identity standards, to provide a federated single sign-on and attribute exchange framework. Using Shibboleth-enabled access simplifies management of identity and permissions for organizations supporting users and applications.

Shibboleth is deployed by a lot of universities, research centers and government agencies in France and in Europe.

In the Shibboleth architecture, UCOPIA works as a Service Provider. Through the UCOPIA portal, the UCOPIA controller allows to redirect the user to the Discorevy Service, then the user can choose his or her own organization. Once the organization selected, the user is redirected to his or her Identity Provider in order to authenticate with his or her organizational credentials.

By default, UCOPIA works with avec the RENATER Discovery Service but can be configured to work with other services.

The schema below describes interaction between the Shibboleh components.

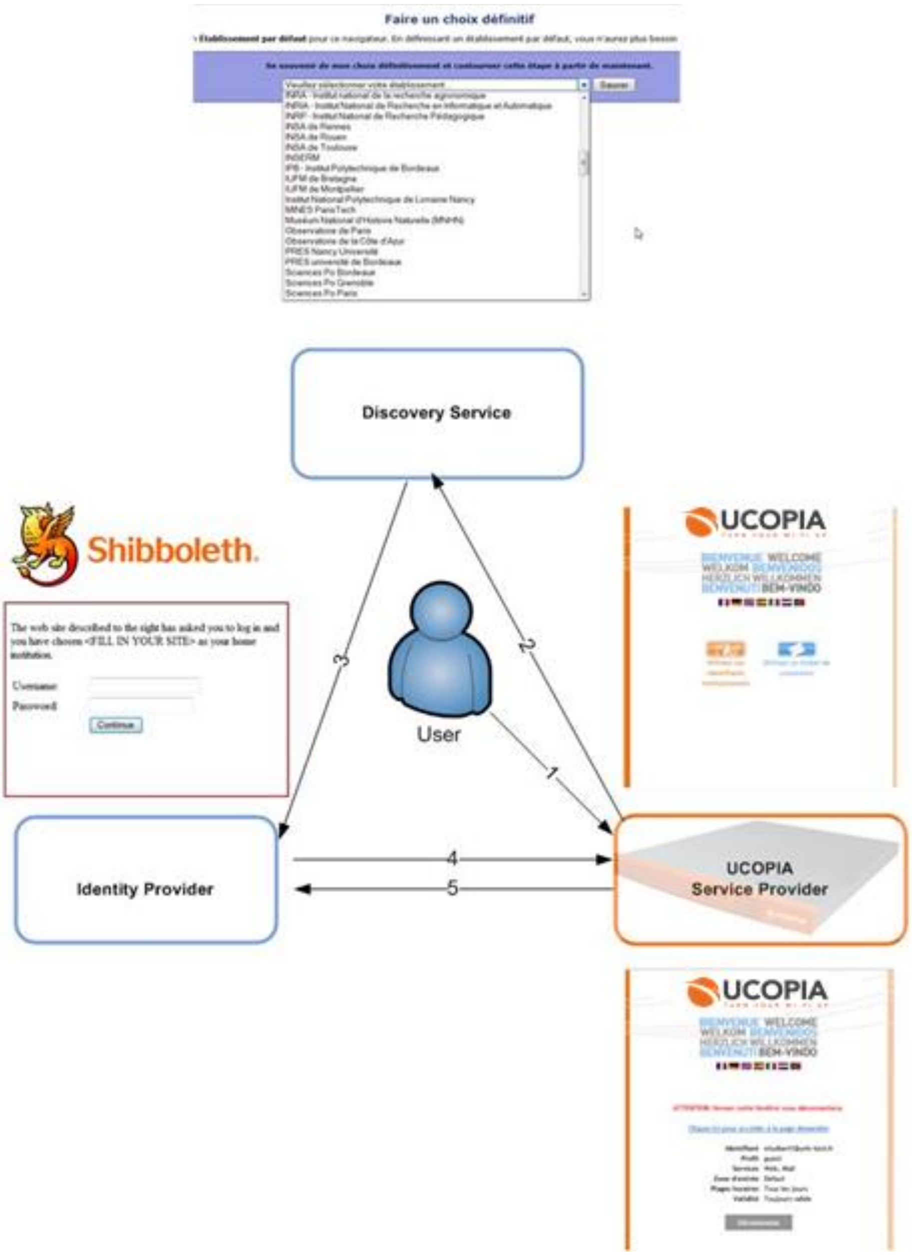


Figure 41: Shibboleth architecture with UCOPIA

5.7 Integration with third party tools

5.7.1 API

To integrate with third party tool (e.g. provisioning or billing solutions), UCOPIA provides an API. For instance, a hospital opens a file for each patient. Besides medical data, the patient may get free and charged services (telephone, video on demand, internet access). The user information is created once only and pushed to each service oriented component including UCOPIA.

The UCOPIA API enables to create, update or remove a user account, associate the user to a predefined profile, based on an HTTP query:

http://<@IP UCOPIA controller>/deleg/api_admin_deleg.php

For instance, to create an account with the "jdupond" login name and the "guest" profile, the API command is:

http://10.0.0.1/deleg/api_admin_deleg.php?deleg_id=deleg&deleg_pwd=deleg&action=adduser&user_id=jdupond&user_pwd=dupond&user_grp=guest

The architecture is the following:

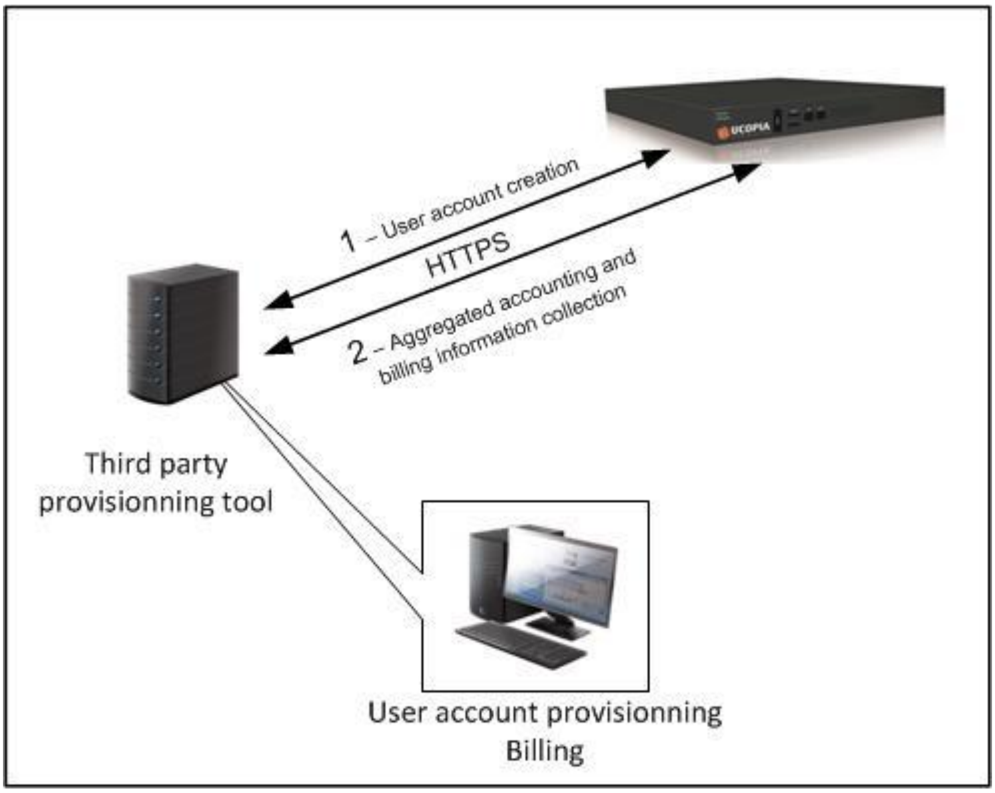

1 – User account creation
HTTPS
2 – Aggregated accounting and billing information collection
Third party provisionning tool
User account provisionning
Billing

Figure 42: Integration with third party tool

5.7.2 Setting up the connection with a PMS (Property Management System)

The UCOPIA controller offers on top of his generic interface API, a dedicated interface for PMS solutions. PMS are customer management solutions, mostly found in hotels or hospitals. Some of their functionalities are customer management, billing…

The connection between an UCOPIA controller and a PMS server is possible with the FIAS protocol and a subscription, defined by the administrator. It could be 1 hour, 3 hours, for emails only or with a VPN access, from 6 to 8, the options are endless. The end user just has to select the subscription he desires and UCOPIA sends to the PMS which option was chosen.

The exchange between UCOPIA and a PMS is as follow:

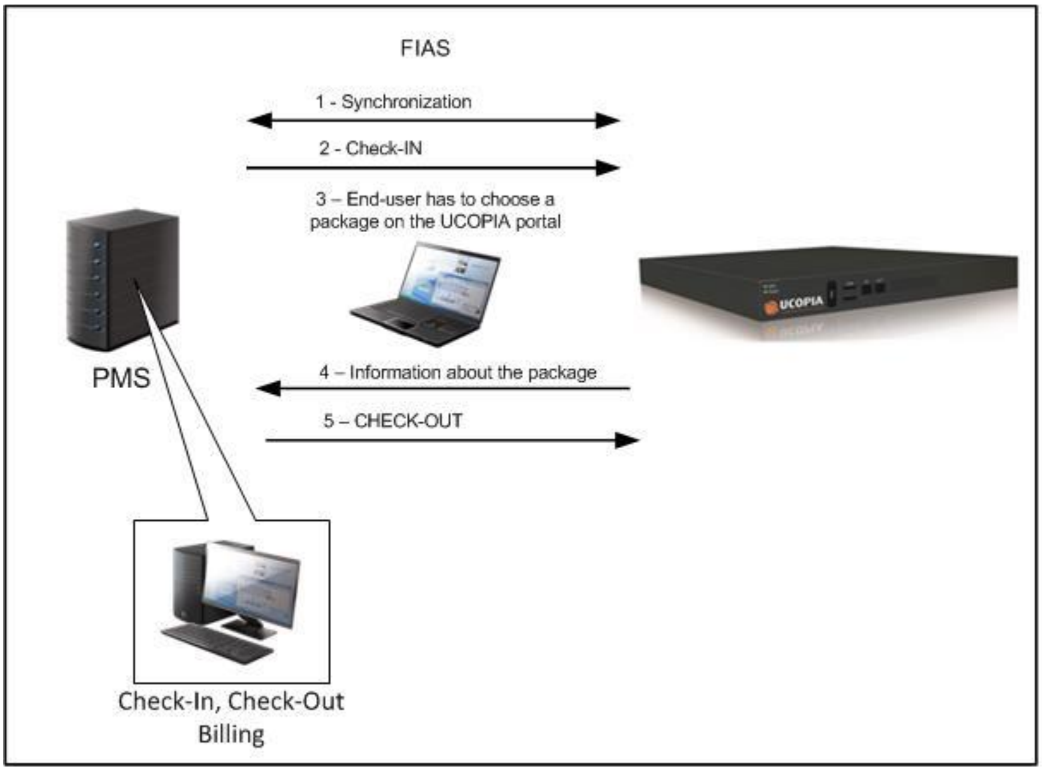

FIAS
1 - Synchronization
2 - Check-IN
3 – End-user has to choose a package on the UCOPIA portal
PMS
4 – Information about the package
5 – CHECK-OUT
Check-In, Check-Out
Billing

Figure 43: Setting up a PMS

5.7.3 Setting up the connection with a PPS (Pre Paid System)

The UCOPIA controller offers a dedicated interface with products such as PPS working with prepaid cards. The user authenticates on the UCOPIA portal filling the card number and a captcha code. The card number is allowing the user to request for time credits to the PPS server. The PPS allocates time in renewable blocks of N seconds. The user account is automatically created inside the UCOPIA controller. On the portal, users can see the connection time for the card and the amount of time used.

5.7.4 Setting up the connection with iPass solution

iPass unifies the management of remote and mobile devices and connectivity. It provides Internet services to business users working remotely (away from their home office, region or country) by integrating Internet connectivity with management of VPN and other third-party security applications. The typical end-user is a mobile worker with a laptop computer, smartphone or tablet device

UCOPIA is iPass compliant, any iPass user can connect through the UCOPIA controller.

The UCOPIA/iPass architecture is the following:

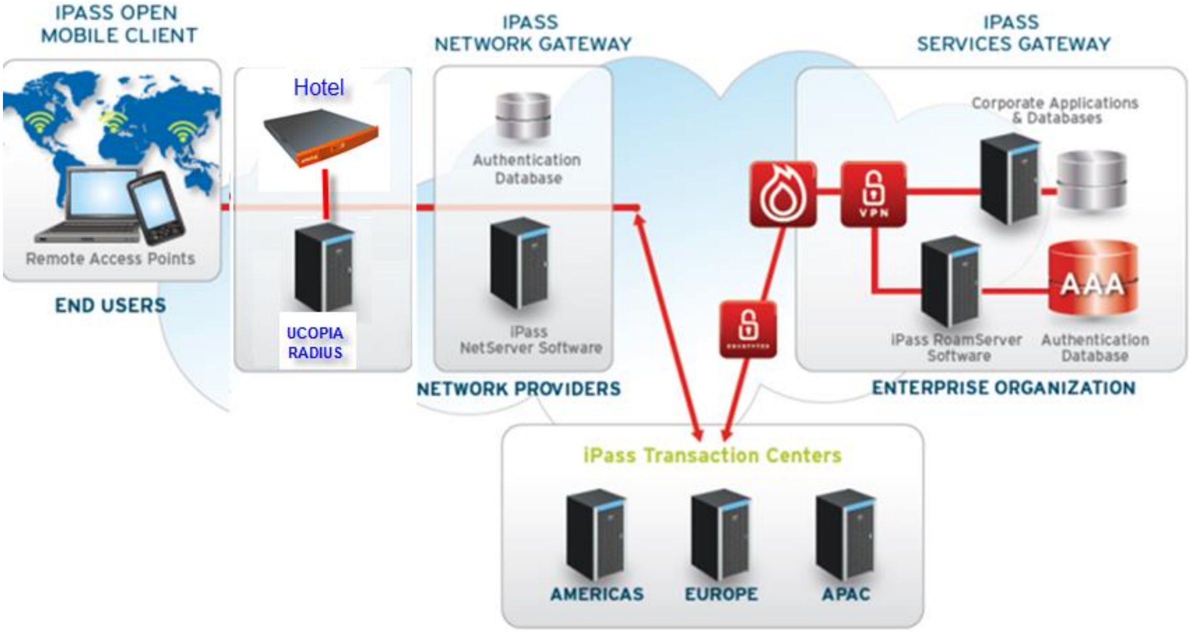


Figure 44: Global UCOPIA/iPass architecture

The UCOPIA controller interacts with the iPass application through the WISPr protocol. Authentication is performed with RADIUS. The RADIUS embedded in the UCOPIA controller is the client of a centralized UCOPIA RADIUS server which works as a proxy to the iPass infrastructure. All RADIUS interactions are done using a VPN.

The schema below describes this technical architecture.

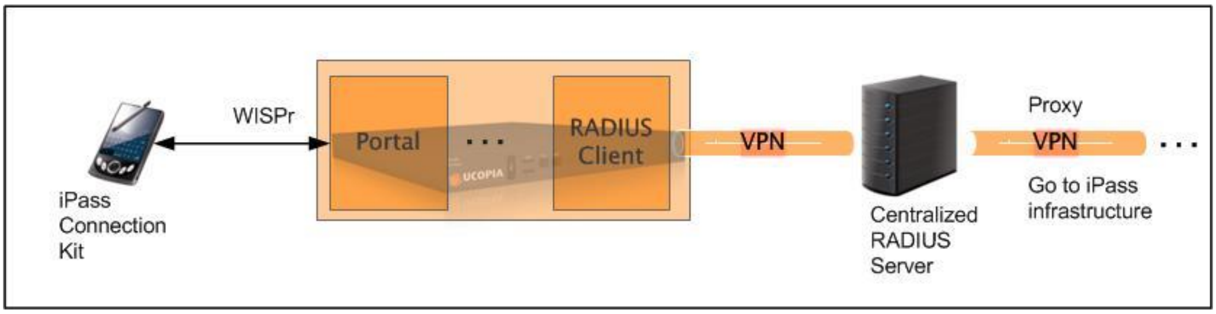


Figure 45: iPass and UCOPIA architecture

6 Network architectures

6.1 Single site architecture

Single site deployments are very frequent in the hospitality or SME markets.

In the case of a hotel, the network infrastructure is simple: internet access through a DSL router and a Universal Thread Management (UTM) device to protect from Internet threats (virus, attacks, etc.). UCOPIA works as a gateway between the rooms and the Internet router (see schema below).

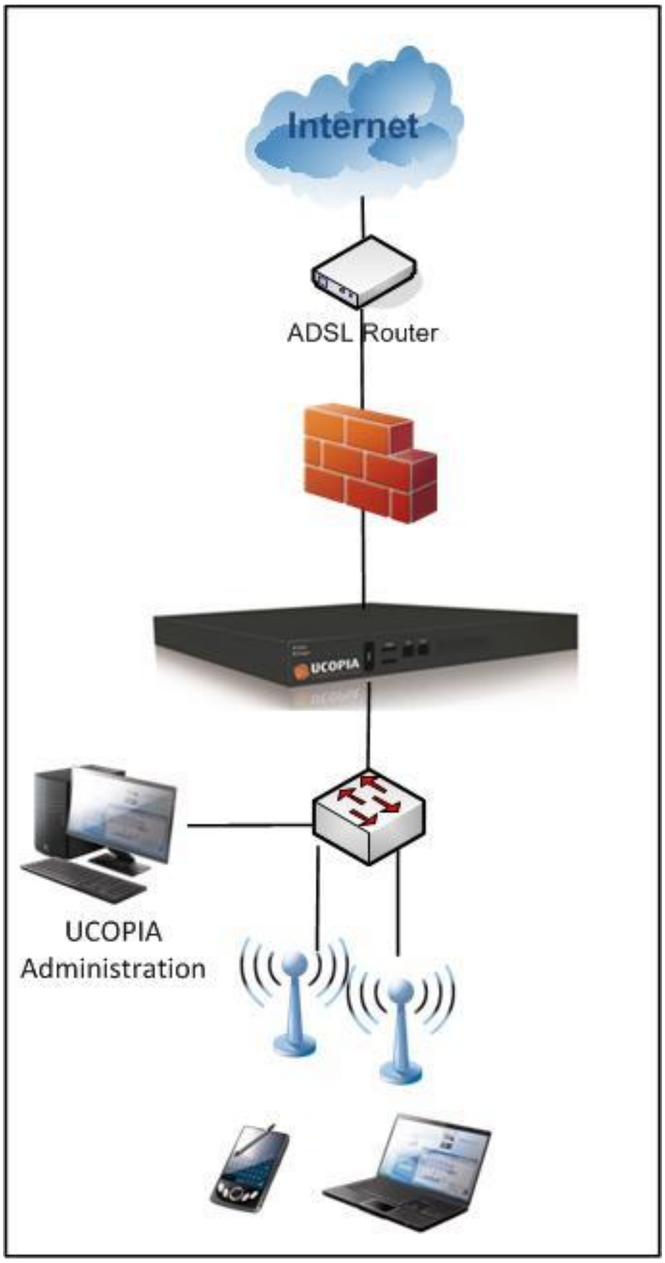


Figure 46: Single site, hotel like architecture

With SMEs, architecture is a little richer, with a directory to store employees accounts, and some VLANs.

The typical UCOPIA architecture in this case is as follows:

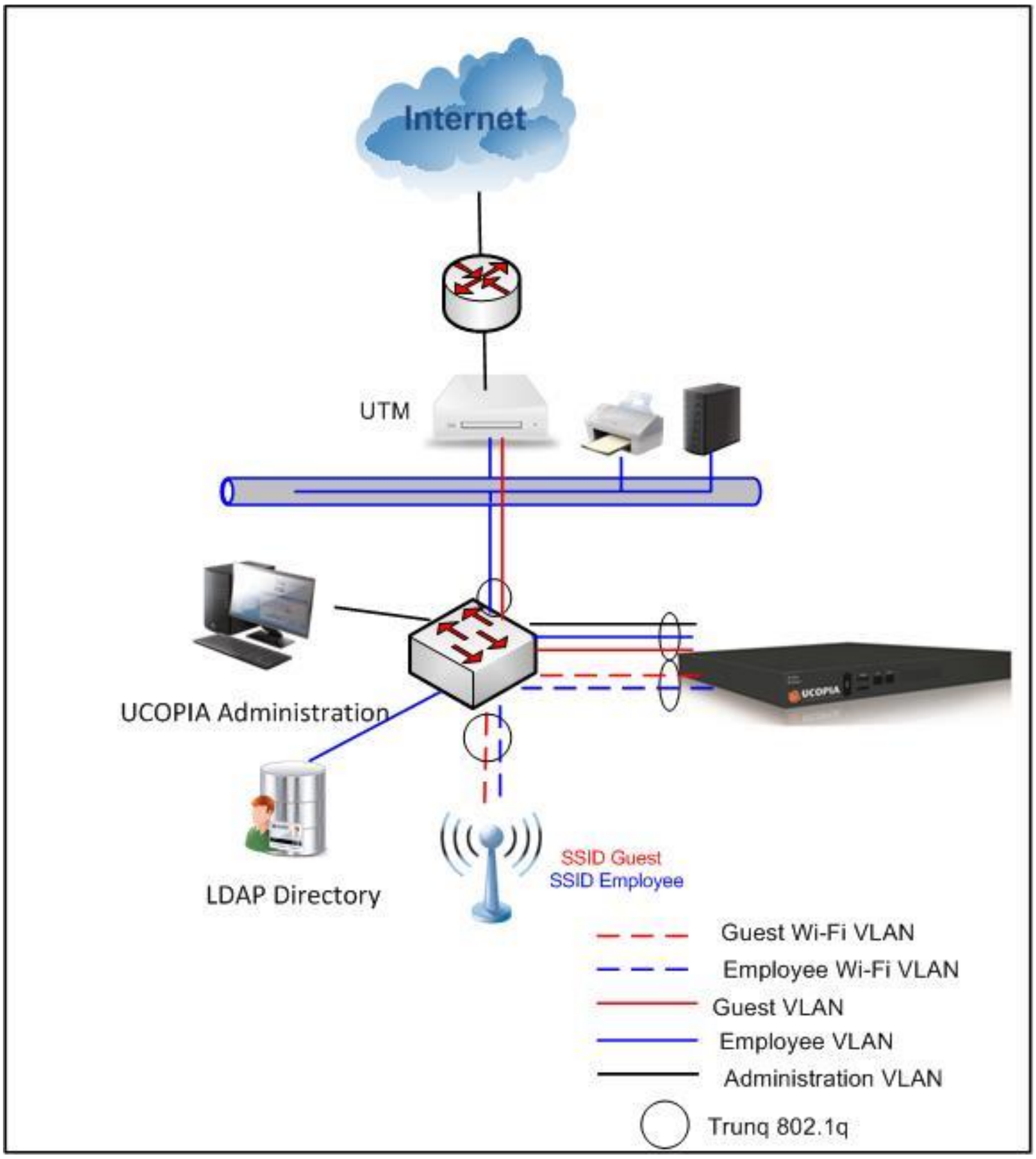


Figure 47: Example No. 2 of single-site UCOPIA architecture

Several SSID/VLAN pairings are defined on Wi-Fi access points in order to isolate different populations of user (guests, employees, etc.). These VLANs are also configured as incoming on the UCOPIA box (802.1q Ethernet card). During the user authentication process, the UCOPIA box can offer separate and appropriate authentication methods on the basis of the type of user, e.g. Web portal for guest users, the 802.1x protocol for employees. In terms of employee authentication, UCOPIA can query the corporate directory (LDAP, Active Directory). Lastly, when exiting the UCOPIA box, user traffic can be redirected to a particular VLAN on the LAN side (the choice of VLAN will be made on the basis of the user profile).

6.2 Multiple sites architecture

Multi-site architectures are usually encountered in large organizations or large companies (major customers, universities, regional student support centers, hospitals, etc.).

The UCOPIA architecture for a multi-site environment can be built with one or more UCOPIA boxes. The box or boxes can either be centralized on one site, or distributed across different sites depending on network connection constraints between sites. UCOPIA enables flexible architecture enables to deploy various architectures scaling from a fully centralized architecture (UCOPIA controllers are based in a single central location but control all APs) to a fully distributed architecture (one controller per location). Centralized architecture delivers ease of management while distributed architecture reduces traffic, improves performance and availability. UCOPIA can fit to these different architectures with large load balanced controllers farm to cope with fully centralized architectures or fully distributed one per location multi-controllers architectures. The following of this section describes these different architectures.

6.2.1 Centralized architecture

In a centralized multi-site architecture, the controller will be centralized on one site and provide service to all remote sites.

The user traffic will be centralized in order to use the centralized Internet access. Centralization of traffic can occur in different ways. Either by traffic routing between the remote site and the central site or by establishing a tunnel (layer 2 or 3) between the remote site and the central site or, in the case of a Wi-Fi architecture type "thin AP", using LWAPP tunnels or CAPWAPP between Wi-Fi access points located on the remote site and the Wi-Fi controller on the central site.

Case of a centralized architecture with routed network (L3) between the remote sites and the central site

If we want, in a routed architecture, to make available UCOPIA features requiring MAC address such as automatic MAC address authentication or 802.1x authentication, that involves that an active equipment can relay DHCP requests and of course that the DHCP service is provided by the UCOPIA controller.

Nevertheless persist to this architecture two restrictions: (1) the client devices at the remote site must be configured in DHCP mode, (2) load balancing requires that layer 3 equipments can be configured to distribute traffic on different controllers cluster (e.g., source routing). If these restrictions are not desired, it is then necessary to establish a layer2 tunnel between the remote site and the central site.

It should be noted that the UCOPIA central controller can be configured to operate in both switched and routed communication.

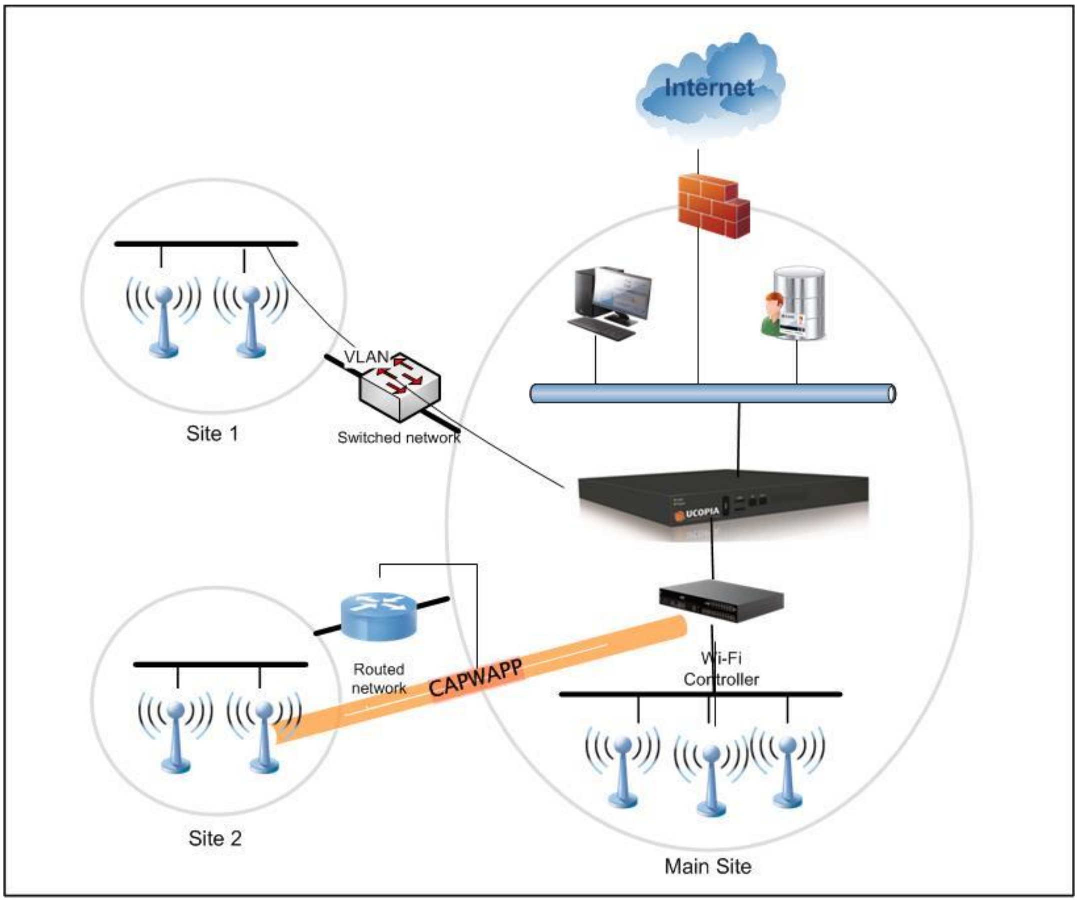


Figure 48: Centralized multi sites architecture

6.2.2 Partially centralized architecture

It is possible to centralize certain services, namely captive portal and authentication. An UCOPIA controller, called Edge, will be present at each site responsible for controlling user traffic and a central controller will deliver portal and authentication features.

In this architecture, user traffic is managed locally at each site and local Internet access is used. UCOPIA Edge controller performs a redirection portal to central UCOPIA, authentication is done through RADIUS protocol. The user directory is located on the central controller.

The advantage of this architecture is to share the authentication portal and the user directory across all sites. This simplifies administration including when updating the portal. In addition, to further simplify administration, UCOPIA Edge controller ensures synchronization of zones, user profiles and other components between the central controller and the Edge. The configuration thus operates only on the central controller.

It should be noted that this architecture can work only with a Wi-Fi infrastructure at the remote site (i.e. without controller UCOPIA). Nevertheless requires that the Wi-Fi solution is compatible with portal redirection protocol and RADIUS. In this case, there is no synchronization mechanism with the central controller.

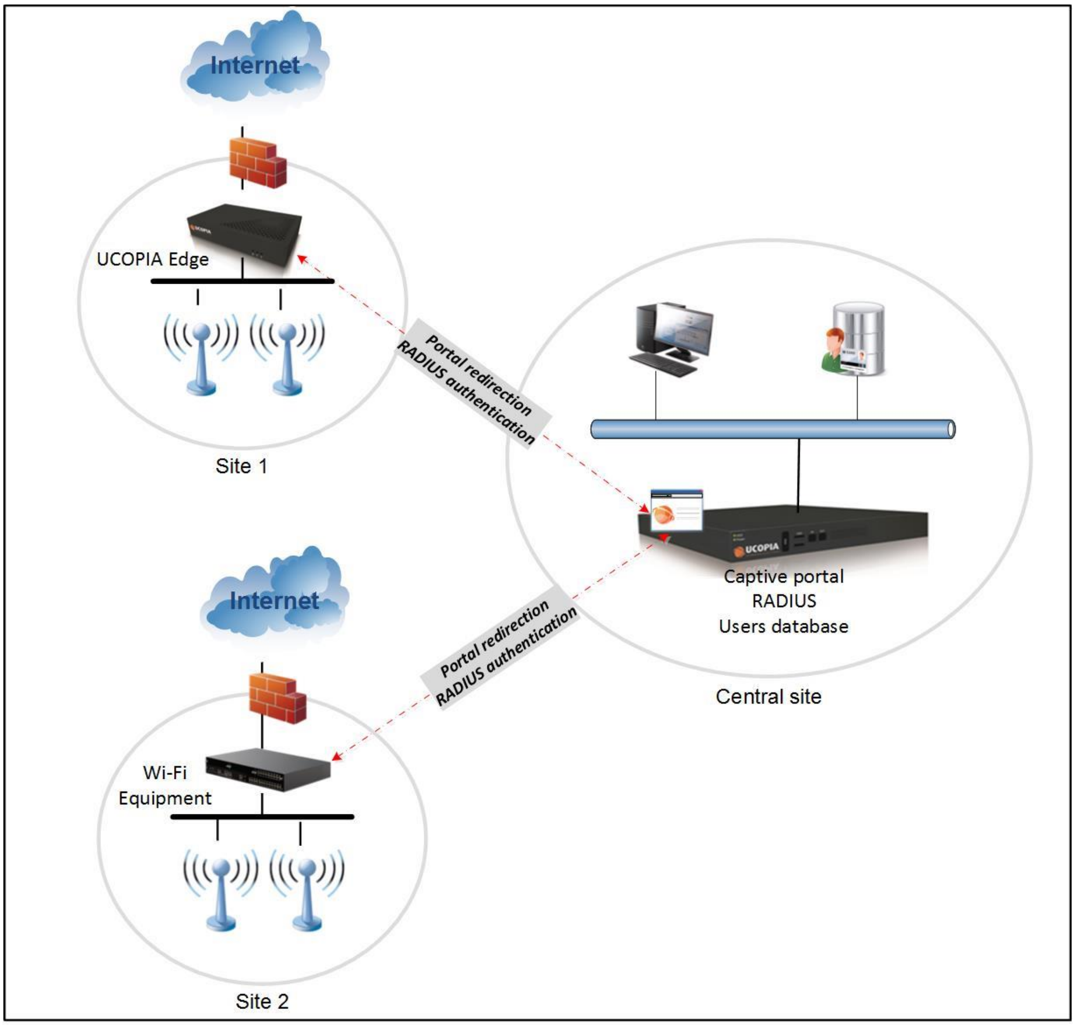


Figure 49: Partially centralized multi sites architecture

6.2.3 Mixed architecture

Architectures described in previous Sections can be combined, consequently some sites can refer to a central UCOPIA while others have their own local controller.

6.3 Multiple zone architecture

UCOPIA uses a "zone" concept in order to describe a certain place. For example, in a company, it could be a reception area or office; at a university, the library or lecture halls.

Zones can be used for security and/or mobility purposes. To enhance security, you can specify if a user population is permitted or forbidden to connect to a certain zone. For example, visitors to a company are not allowed to connect to the office zone, but only to the reception zone. In the case of using zones in a mobility context, you can set up a different captive portal for each zone. You can also define different usage rights for users according to their connection zone. For example, you can allow a company employee to connect to all zones without any time restriction, and to be accepted in the company reception zone, where their connection time will be limited.

There are incoming and outgoing zones; the respective entrance and exit points are related to the UCOPIA appliance and its separation-based architecture.

From a network perspective, incoming zones correspond to subnets. In a local area network architecture (layer two), the zones correspond to VLANs; in a remote network architecture (layer three), the zones will correspond to subnets. Outgoing zones in all cases correspond to VLANs. The incoming zone/subnet correspondence occurs during the configuration of the incoming networks at the level of the UCOPIA controller. In respect to outgoing activities, the zones are associated with a user profile.

In the example below, a student profile will be configured to allow the connection to the "library" and "cafeteria" incoming zones. Users are prohibited from connecting to the "Administration" zone, therefore the respective connection will not be configured in the profile. On the website below, Library = VLAN 2 + VLAN 3. On another site, the Library zone could be implemented using other VLANs.

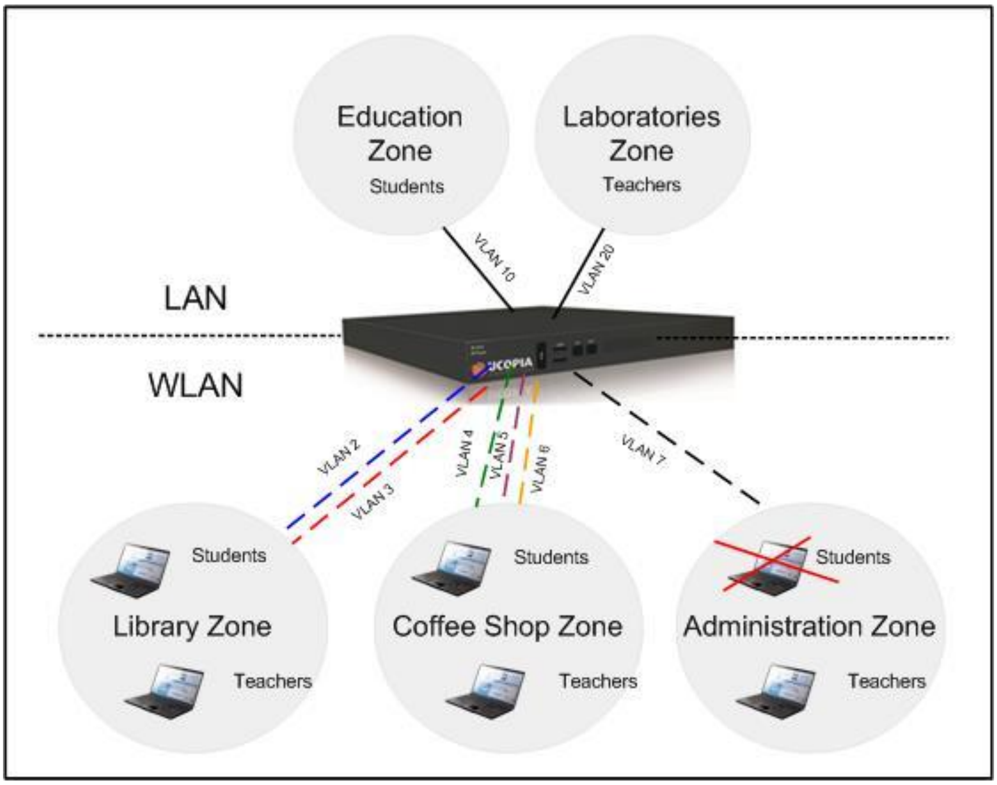


Figure 50: Multi zones architecture

In a multi-site architecture with centralized administration, a zone is a global concept, and is interpreted in the same way by all the UCOPIA boxes at all the sites. On the other hand, the way in which zones are set up is specific to each box. The link between zone and VLANs is established when each box is configured. Not all zones are necessarily defined for each box.

6.4 Cloud architecture

UCOPIA offers different architectures, centralized, distributed or mixed (see previous Sections) for deploying highly flexible Cloud architectures.

It should be noted that Cloud architectures are deployed and operated by UCOPIA’s partners in their infrastructures.

The following diagram summarizes the various possibilities of architectures in the cloud.

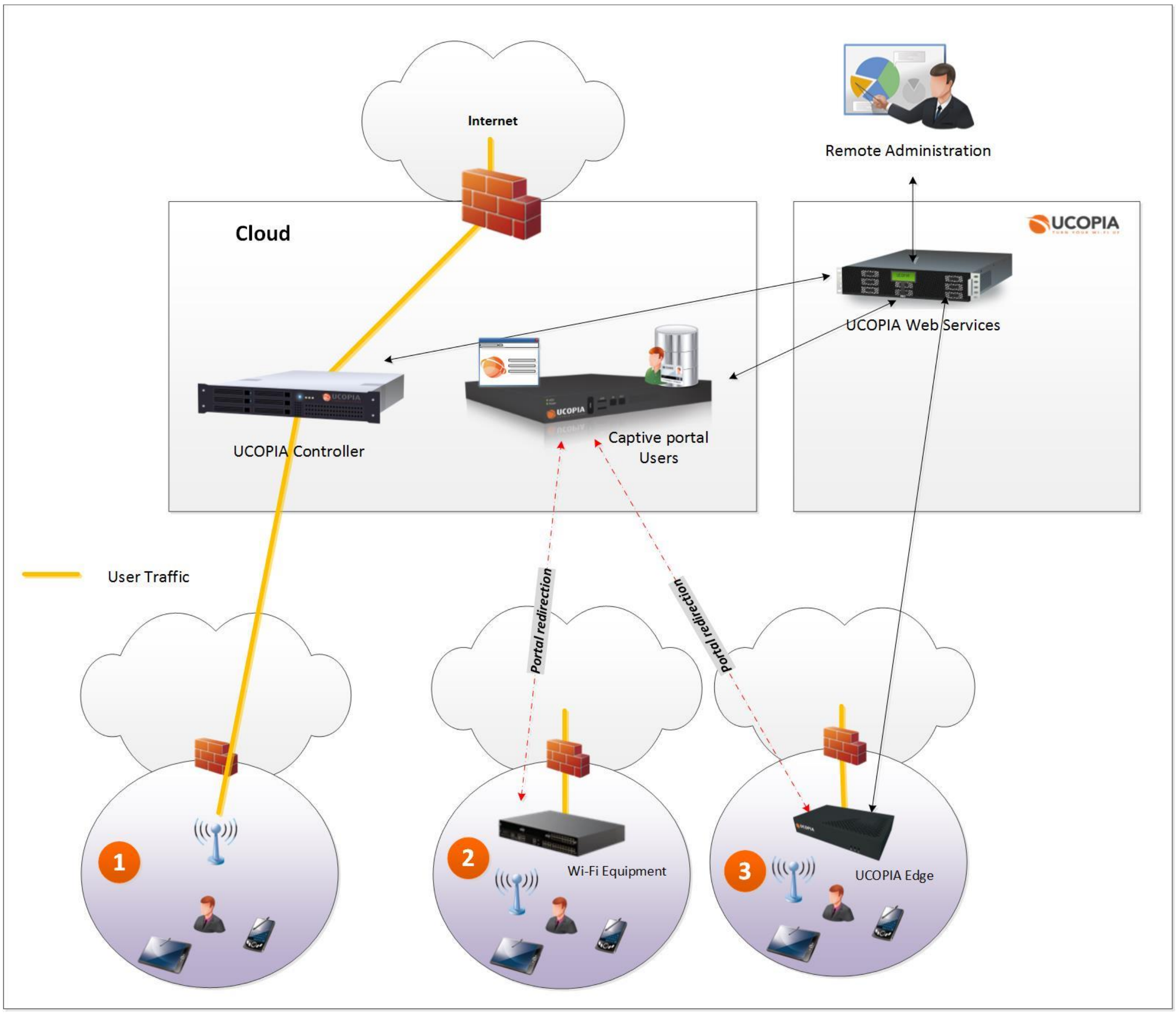


Figure 51 : Cloud architecture

- **Case N°1 : "Inline" centralized architecture**

  User traffic is centralized in the cloud, the Internet access is at the Cloud. All UCOPIA functions are provided by one (or more) UCOPIA controllers in the Cloud. This architecture meets the needs of operators, WISP or big chain of stores.

- **Case N°2: "Out-of-band Vendor" centralized architecture with on-premise Wi-Fi equipments.**

  The captive portal, authentication and user directory are centralized, the user traffic is not centralized (out-of-band). This architecture allows to deport some UCOPIA controller features in the cloud allowing centralized management of these functions. Wi-Fi equipment ensures redirection to the centralized UCOPIA portal and authentication (RADIUS exchange with the UCOPIA RADIUS server).

  This architecture has the advantage of not requiring the addition of components to the local site outside of Wi-Fi equipment. In terms of traceability, user sessions logs are available in the Cloud and according to the Wi-Fi vendors, other information can be centralized in the Cloud (e.g. visited URLs).

  This architecture meets the needs of operators, WISP for small and medium market. Or for multiple points of sales of a retail chain.

- **Case N°3: "Out-of-band Edge" centralized architecture with on-premise UCOPIA Edge.** This is comparable to the architecture N°2 but with a UCOPIA controller on local site. Due to the presence of an inline UCOPIA controller on site, this architecture allows to provide all UCOPIA features such as user traffic log, URL filtering or Web Injection. An automatic synchronization (zones, profiles, etc.) is automatically performed between the central controller and the Edge controllers.

6.5 Multi-tenant architecture

In a centralized architecture, the central controller can serve several sites or customers, this controller can then operate in multi-tenant mode. In this mode each site must be associated with a network perspective to one (or more) incoming zone (s). This will make it possible to customize the controller depending on the zone and possibly the user profile. For example, the license in terms of simultaneous connections may be splitted by site, a personalized portal can be different for each site. Other features will be applicable depending on the zone and therefore the site, such as reporting statistics, delegation portal, connection ticket, etc.

Note that the UWS services can also be used in multi-tenant mode, so Wi-Fi Marketing can achieve Web injection for a profile associated with a zone, Wi-Fi Marketing can operate on the data of one or several zones.

The following diagram illustrates this multi-tenant architecture

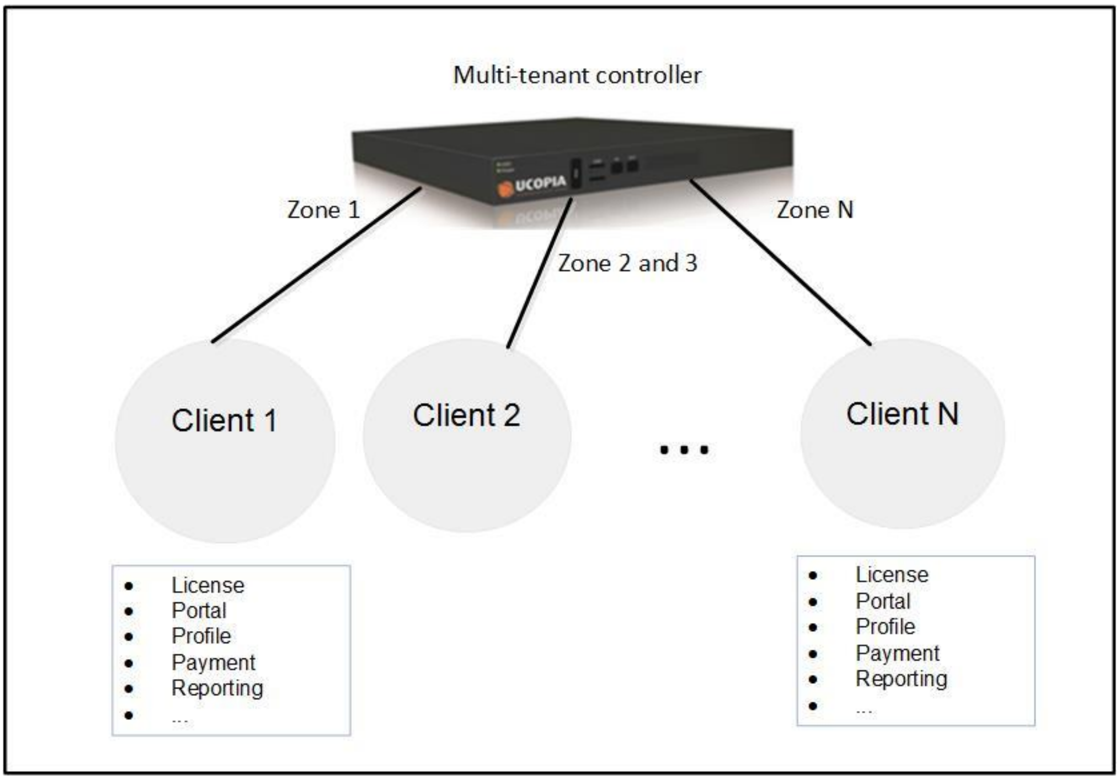


Figure 52: Multi-tenant architecture

7 UCOPIA High availability

To face availability and scalability requirements, UCOPIA implements redundancy and load balancing features. This enables serving thousands of concurrent users and delivering nonstop operation in case of hardware failure.

UCOPIA also offers a load balancing mechanism allowing multiple UCOPIA boxes to balance user connections. Redundancy and load balancing are two independent and complementary mechanisms.

7.1 Redundancy

UCOPIA redundancy is based on an Active controller / Passive Controller model. The UCOPIA boxes used in a redundancy architecture are in communication and, consequently, each registers any failure of the other.

Failover of one UCOPIA box to the other takes place thanks to a virtual IP address. In fact, at any given moment, only one controller has the virtual address. In case of failure of the active controller the redundant controller detects failure through the VRRP protocol and gets the virtual IP address. Then, the passive controller becomes active. This mechanism is totally transparent for the end user.

In a redundancy architecture, as in a multi-site architecture, we find a Principal controller and a Secondary controller. Any modification done on the UCOPIA directory of the main controller is automatically replicated on the Secondary controller.

Active and passive controllers must be on the same VLAN.

The diagram below illustrates redundancy architecture.

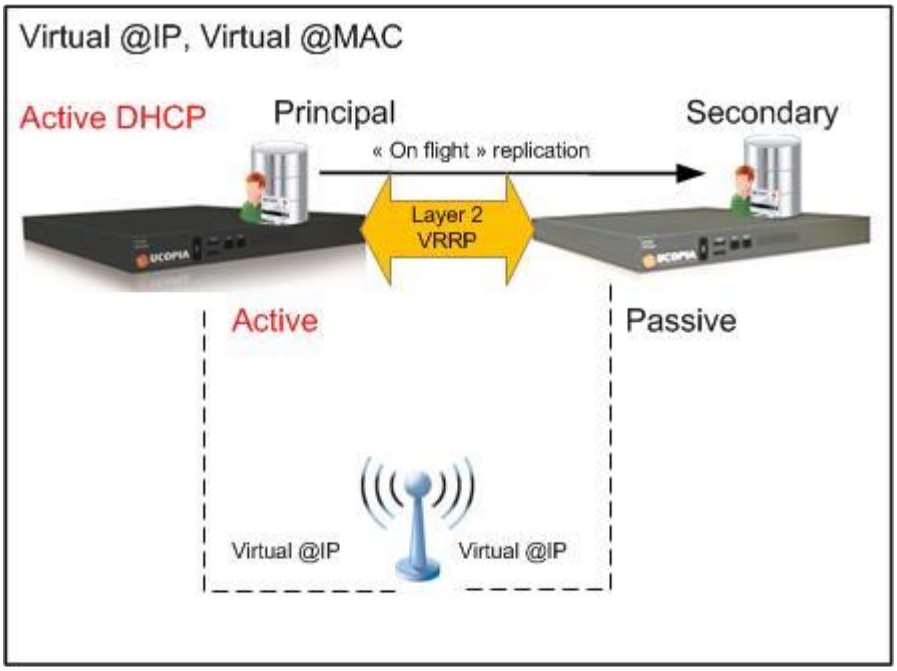


Figure 53: Redundant architecture with UCOPIA

7.2 Load balancing

Load balancing allows to share out equitably user connections on several controllers.

As redundant architecture, load-balancing mechanism works with the VRRP protocol in order to communicate between controllers and uses virtual IP and MAC addresses. The DHCP server is only activated on the Principal controller.

UCOPIA directory is dynamically replicated across all others controllers.

The schema below shows 3 load balanced controllers and a redundant controller. The redundant controller is in charge of the redundancy for the 3 active controllers.

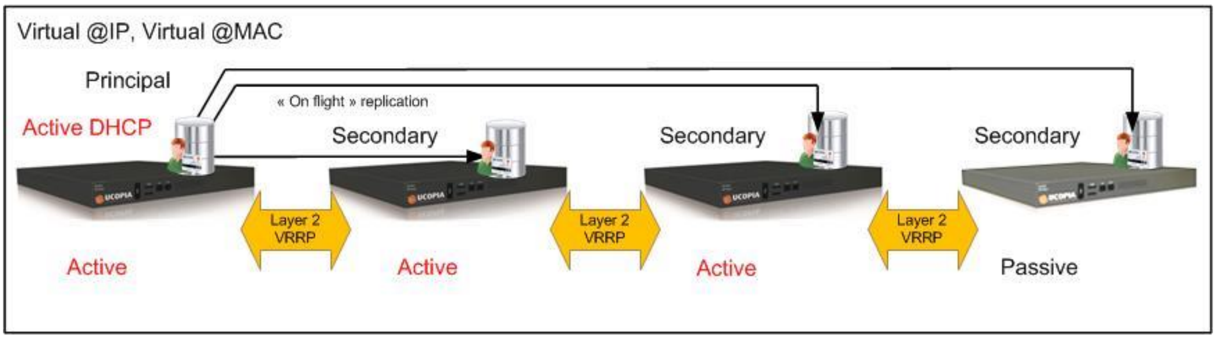


Figure 54: UCOPIA load balancing architecture

8 UCOPIA Web Services platform

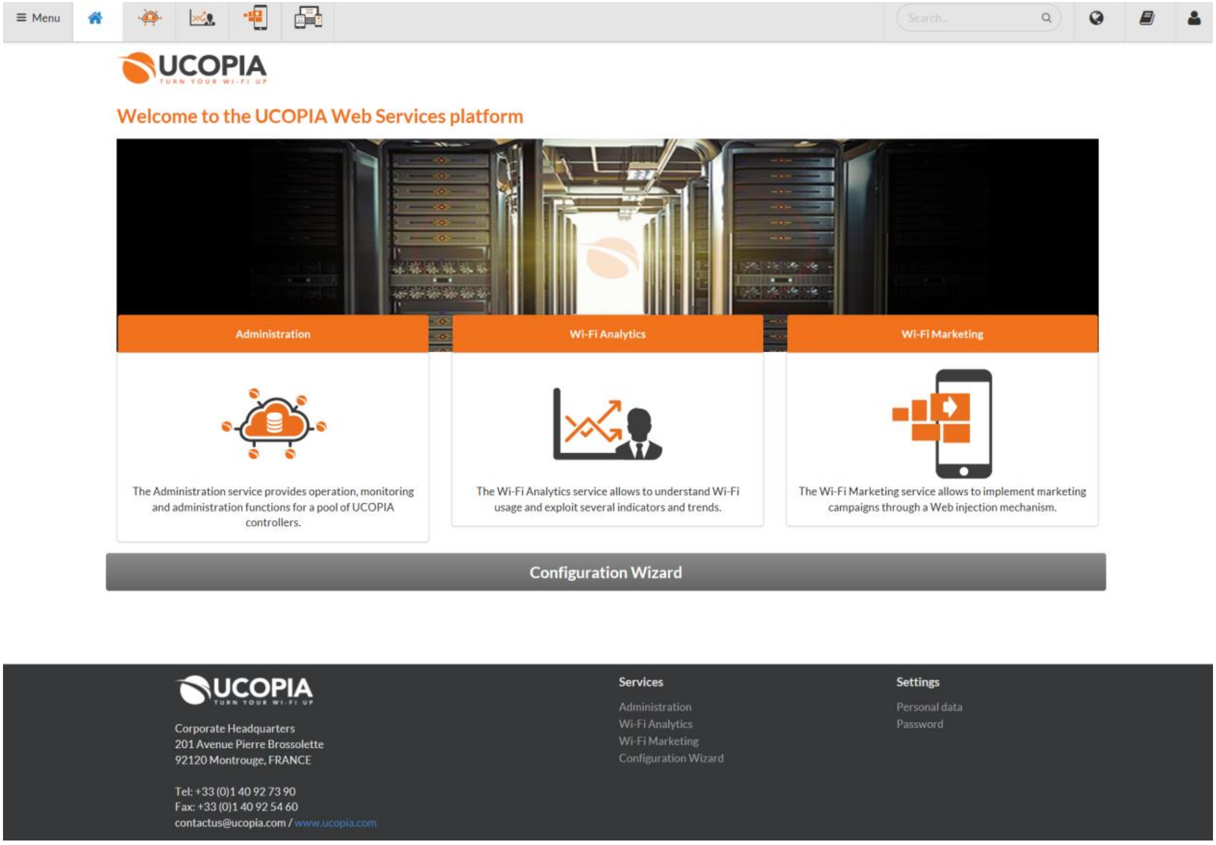
The platform UCOPIA Web Services (UWS), hosted by UCOPIA, is dedicated to customers and partners and offers operating, supervision and administration of UCOPIA controllers, and analytics and marketing services.

To take advantage of these services will require that controllers are configured to allow communication with UWS platform (see Section Architecture).

Three main services are available on top of UWS.

- Administration
- Wi-Fi Analytics
- Wi-Fi Marketing

A configuration Wizard allows to create Smart configurations that can be deployed on one or several remote controllers.



Welcome to the UCOPIA Web Services platform

Administration

The Administration service provides operation, monitoring and administration functions for a pool of UCOPIA controllers.

Wi-Fi Analytics

The Wi-Fi Analytics service allows to understand Wi-Fi usage and exploit several indicators and trends.

Wi-Fi Marketing

The Wi-Fi Marketing service allows to implement marketing campaigns through a Web injection mechanism.

Configuration Wizard

Corporate Headquarters
201 Avenue Pierre Brossolette
92120 Montrouge, FRANCE

Tel: +33 (0)1 40 92 73 90
Fax: +33 (0)1 40 92 54 60
contactus@ucopia.com / www.ucopia.com

Services
Administration
Wi-Fi Analytics
Wi-Fi Marketing
Configuration Wizard

Settings
Personal data
Password

Figure 55: UCOPIA Web Services – Home page

8.1 UWS Administration

The Administration service provides operation, monitoring and administration functions for a pool of UCOPIA controllers.

8.1.1 Operations

In terms of operations, UWS provides the following services.

8.1.1.1 Automatic installation of licenses (or updates)

First of all, a license must be installed on the UCOPIA controller.

The UCOPIA license determines the product range (Express, Advance) and the maximum number of concurrent connections (Express 20, Advance 1000, etc.)

License once assigned to a controller can be distributed by the administrator depending on the zones and user profiles. The distribution per zone is useful to associate a license to a place or a site in a multi-site architecture. The distribution per profile allows to reserve a number of licenses for a given type of users.

Once connected on the network, the appliance interrogates, by request of the network administrator, the UWS platform. This platform extracts data from the controller (serial number, etc.) and verify on its information system the validity of the request. Once theses checks done, a license is generated and automatically installed on the UCOPIA appliance.

8.1.1.2 Automatic upgrade delivery

UCOPIA regularly delivers patches and upgrades, the aim of which is to provide bugfixes, enhancements and new features.

Using UWS platform, upgrades are periodically downloaded onto the controller, ready for installation. The administrator is informed and can decide whether or not to install them.

The platform also offers an automatic installation service for corrective upgrade.

8.1.1.3 Automated remote access tunneling

The maintenance tunnel allows UCOPIA engineers to investigate remotely on the UCOPIA controller, for analysis and diagnostics. If needed, the tunnel is going to be activated without any intervention from the system administrator. It is noted that the maintenance tunnel is established from the UCOPIA box to the maintenance servers.

8.1.1.4 Maintenance validity control

An alert warns the administrator when the maintenance validity expires. Once the license has expired, it becomes impossible to get access to the maintenance and to download the update files.

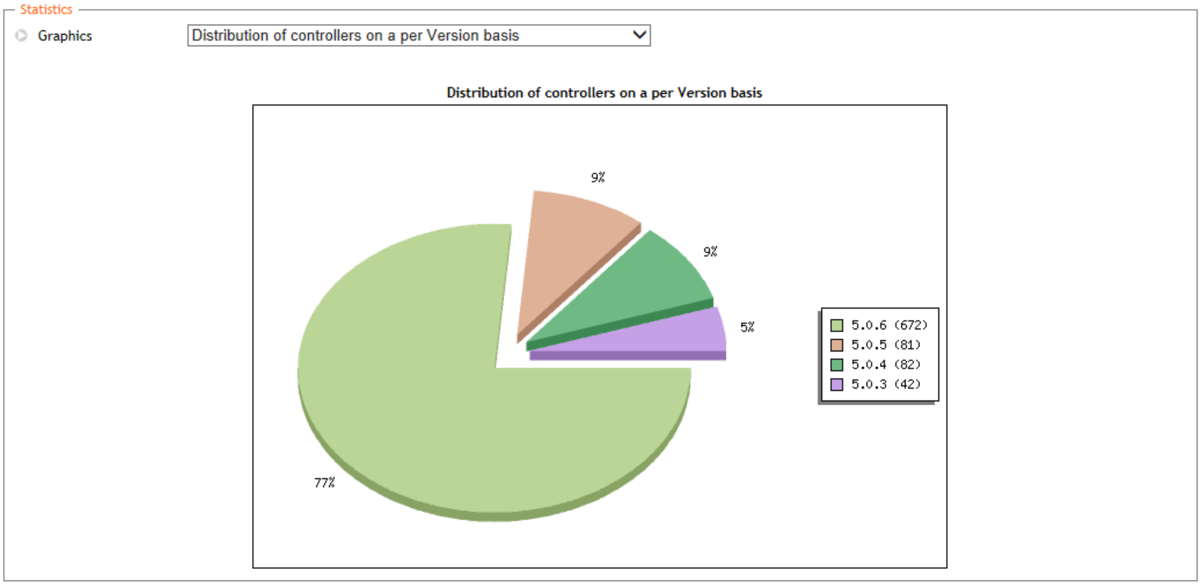
8.1.2 Monitoring and administration

The UWS platform provides additional services dedicated to UCOPIA partners. The objective is that they can monitor and manage all UCOPIA controllers of their own pool.

One of the first functionality of the controller management is to organize the controllers with different criteria, as such as final client, type of product, region, and so on. So, the pool of controllers can be structured with sub-groups of UCOPIA controllers, allowing optimizing the management of the controllers.

Other functions are offered, including the possibility to supervise the controller (temperature, number of simultaneous connections, disk status …) and a quick access to the delegated and administration interface. It is possible to administrate the UCOPIA controller one by one or as a pool of controllers.

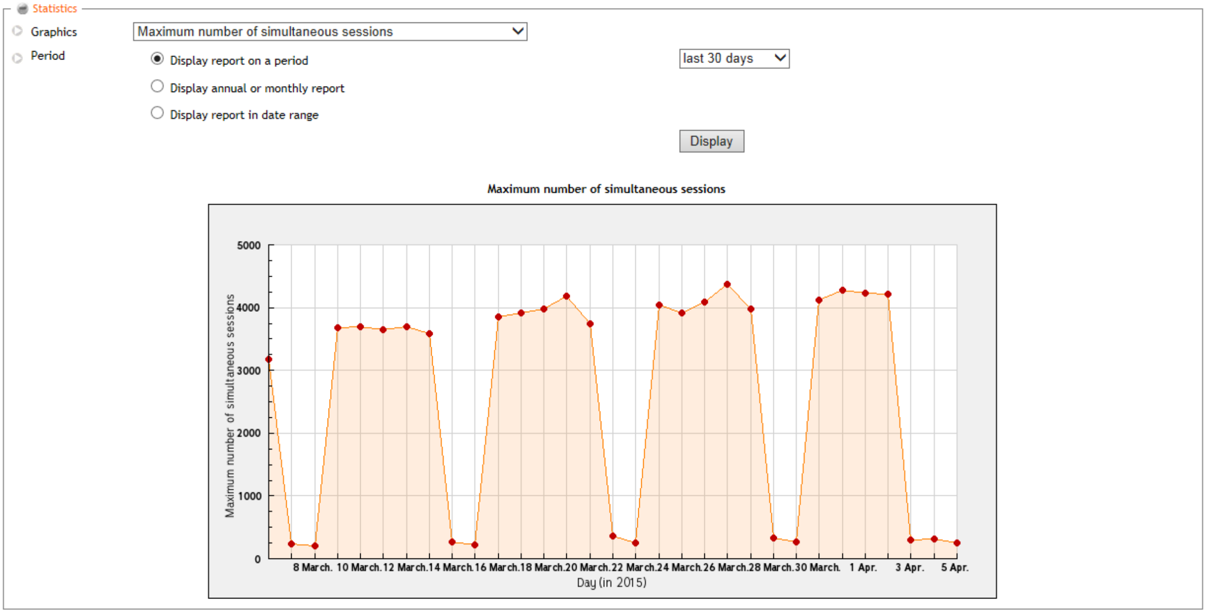
The following screenshot is going to illustrate some of the monitoring features.



Statistics

Graphics: Distribution of controllers on a per Version basis

Figure 56: Global statistics depending on the type of releases installed



Statistics

Graphics: Maximum number of simultaneous sessions

Period:
● Display report on a period — last 30 days
○ Display annual or monthly report
○ Display report in date range

Figure 57: Number of concurrent connections per day

The partner can check the updates and the software level on each controller, upload updates, and apply them on the appliance.

Alerts may be triggered for certain types of event (expiring maintenance contract, disk drive nearly full, controller with abnormally high temperature, etc.). These alerts can be sent to the administrator by email.

8.2 Wi-Fi Analytics: business intelligence and analytics

The UCOPIA controller logs and keeps technical data (the number of simultaneous connections, the number and duration of sessions, etc.) but also information about the users of the solution (who are they?

with what kind of equipment do they connect? what do they do?). The captive portal and the social network connectors contribute to enrich the user knowledge.

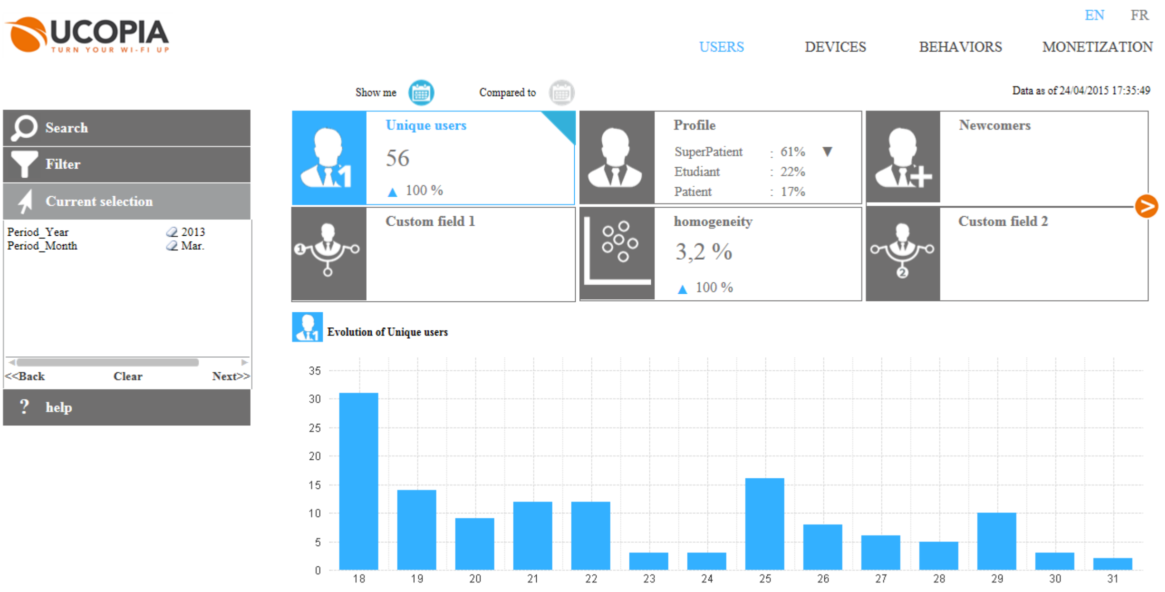
The Wi-Fi Analytics service, available from UWS, allows the owner of the UCOPIA solution to explore all his data in order to get the big picture. It is possible to enter any word or phrase in any order in the search box of the analytic tool to get immediately associative results, to visualize new connections and relationships across data.

The Wi-Fi Analytics service therefore allows to understand Wi-Fi usage and exploit KPI (Key Performance Indicators) and trends. It provides predefined views on users, devices, behaviors and monetization. The service also allows analytics from personal and demographic information (digital marketing).

The Wi-Fi Analytics service makes decision-making easier and, as available in the cloud, it can be used without impacting production.

Data Associations are presented graphically and dynamically through a dashboard.

The page below shows an example of dashboard.



Data as of 24/04/2015 17:35:49

Period_Year 2013
Period_Month Mar.

Unique users: 56, ▲ 100 %

Profile:
SuperPatient : 61%
Etudiant : 22%
Patient : 17%

homogeneity: 3,2 %, ▲ 100 %

Figure 58: Example of analytics dashboard

This service is dedicated to UCOPIA customers in view of the confidentiality of the data handled or to resellers mandated by their customers.

8.3 Wi-Fi Marketing : marketing campaigns and content injection

The purpose of the service Wi-Fi Marketing, available from UWS, is to implement marketing campaigns through a Web injection mechanism. The Web injection consists in injecting content into web pages visited by the end user. The content may be advertising or value-added services. Like the Analytics service, this service is offered to UCOPIA customers and to resellers mandated by their customers.

For example, a hotel can insert a page bottom banner with its logo allowing customers to experience the services of its establishment. The user remains permanently connected to the hotel's services and can be accessed immediately without the need to return to a particular page. This is the guarantee for the hotel manager to optimize the visibility of his services and bring to customers a nice end-user experience in order to consume more and better.

The addition of advertising is another use of the Web injection, it allows to create income from advertisers to the organization that deploys the service.

Once an UCOPIA controller is registered to this service, web traffic (HTTP) user is then redirected to the Cloud so that the injection can be done.

Different kinds of injection are available such as banner, menu, picture, video, link, etc.

The example below corresponds to a hotel that has encrusted bottom of the page a banner to give information about the hotel and forward the user to the hotel website.

The user is looking for a restaurant on Internet. The hotel offers him through his banner to discover the hotel restaurant.

The user clicks on the banner.

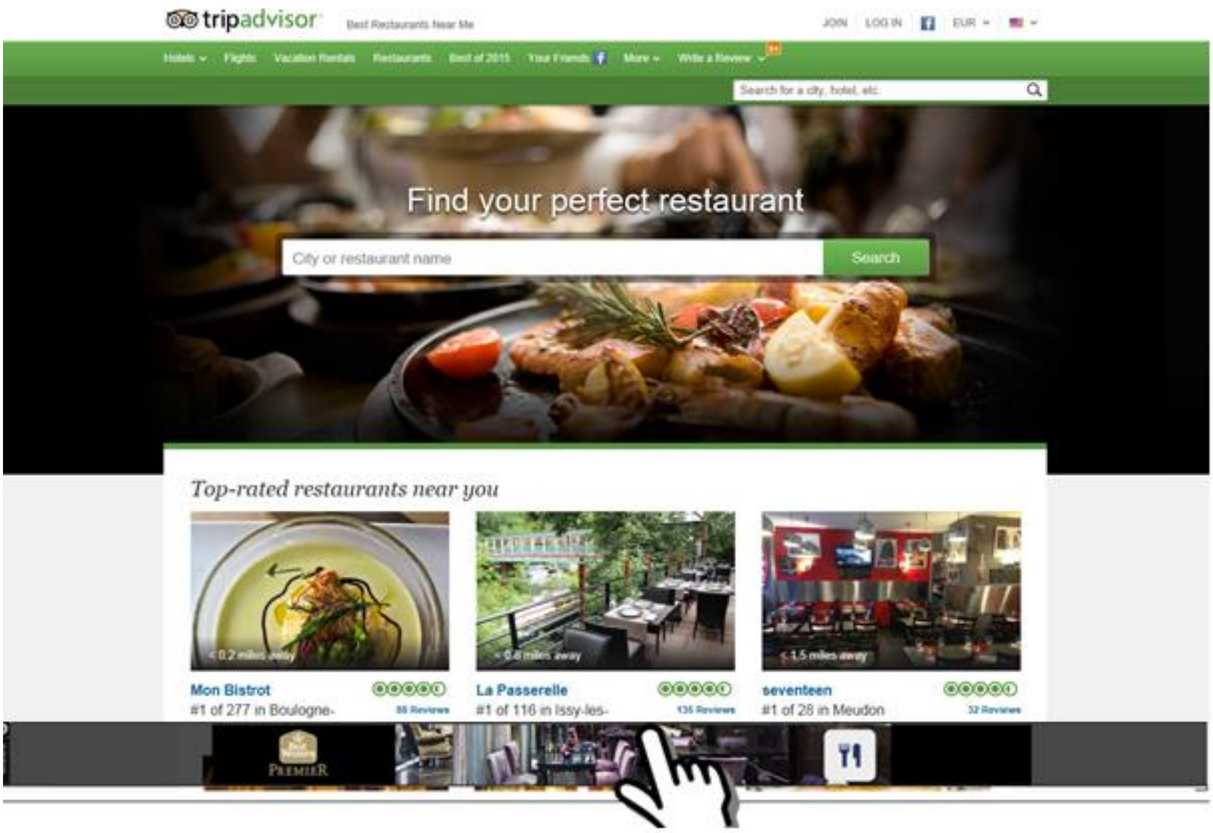


Figure 59: Example of marketing campaign

A popup appears where the user can click to reach the hotel website.

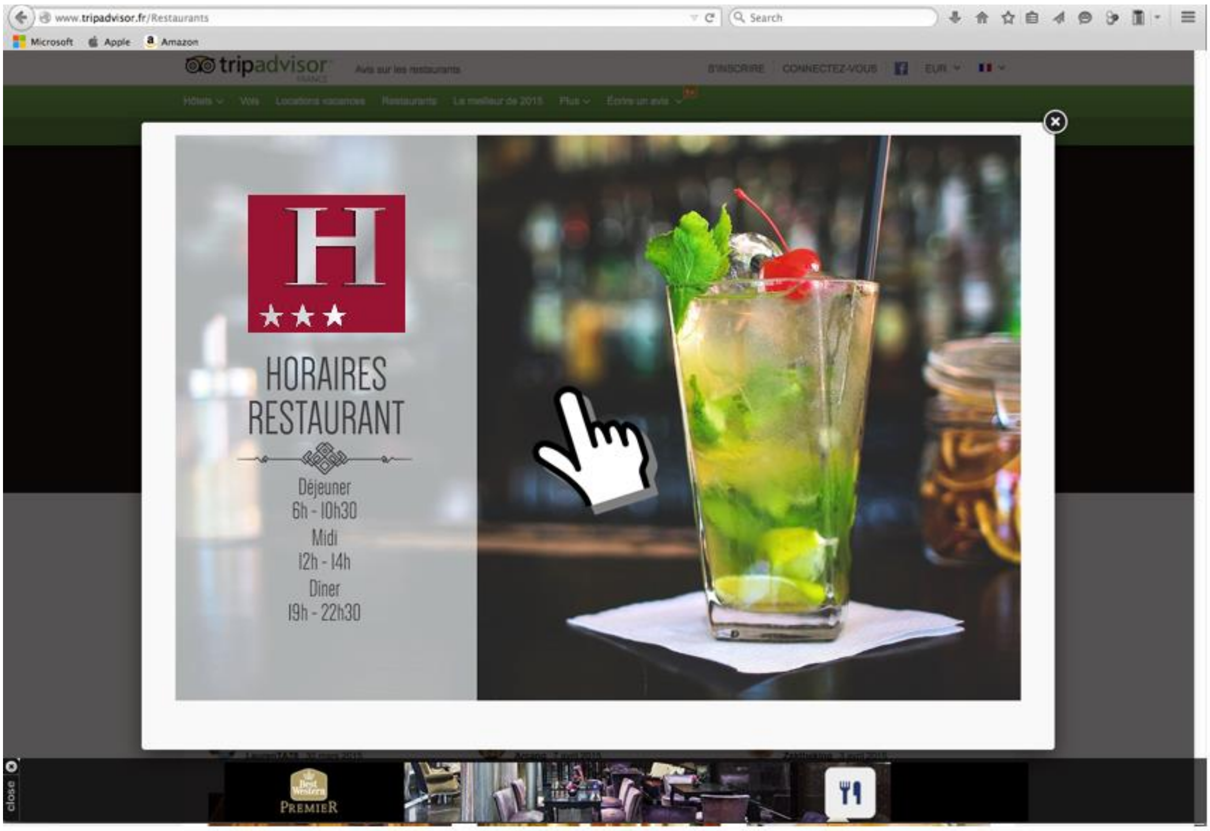


Figure 60: Example of marketing campaign (cont)

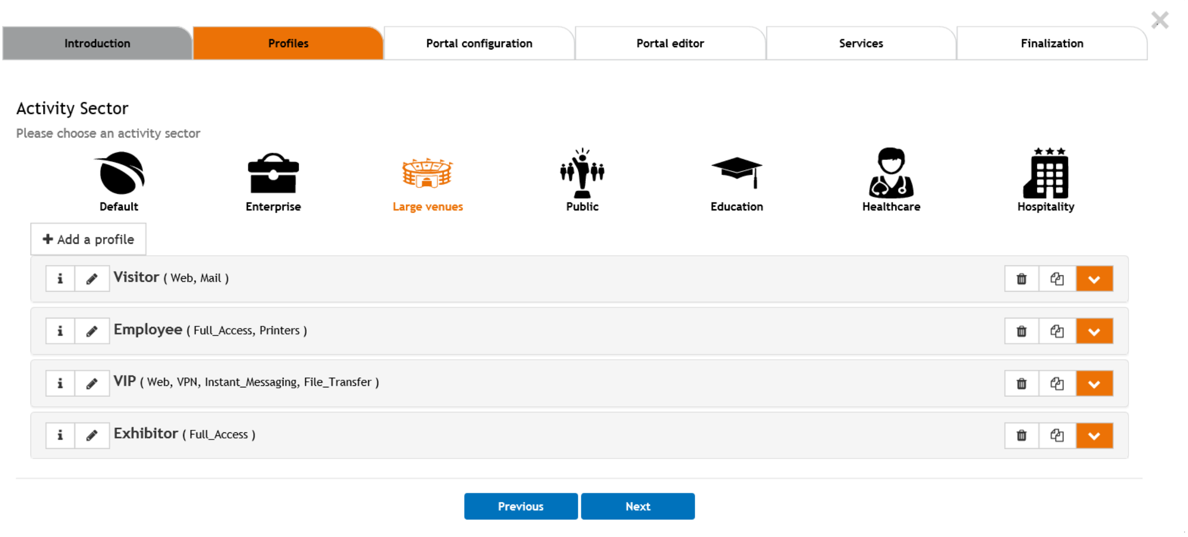
8.4 Configuration Wizard

The configuration wizard allows to create or edit in a very easy way simple and generic configurations (i.e. without network information) called Smart configurations. A Smart configuration defines user profiles with basic parameters (access rights, validity, time credit, filtering, etc.), and portal configurations (authentication via social networks, free registration, etc.) that can be associated to responsive visuals. These Smart configurations can be deployed on one or more controllers in one operation.

Creating a Smart configuration is mainly done in 4 steps:

1. Defining user profiles

The wizard offers a range of activity sectors for which typical profiles are already predefined. For example for the large venues sector, the profiles Visitor, Exhibitor, VIP, and Employee are predefined.



Introduction | Profiles | Portal configuration | Portal editor | Services | Finalization

Activity Sector

Please choose an activity sector

Default | Enterprise | Large venues | Public | Education | Healthcare | Hospitality

+ Add a profile

Visitor (Web, Mail)

Employee (Full_Access, Printers)

VIP (Web, VPN, Instant_Messaging, File_Transfer)

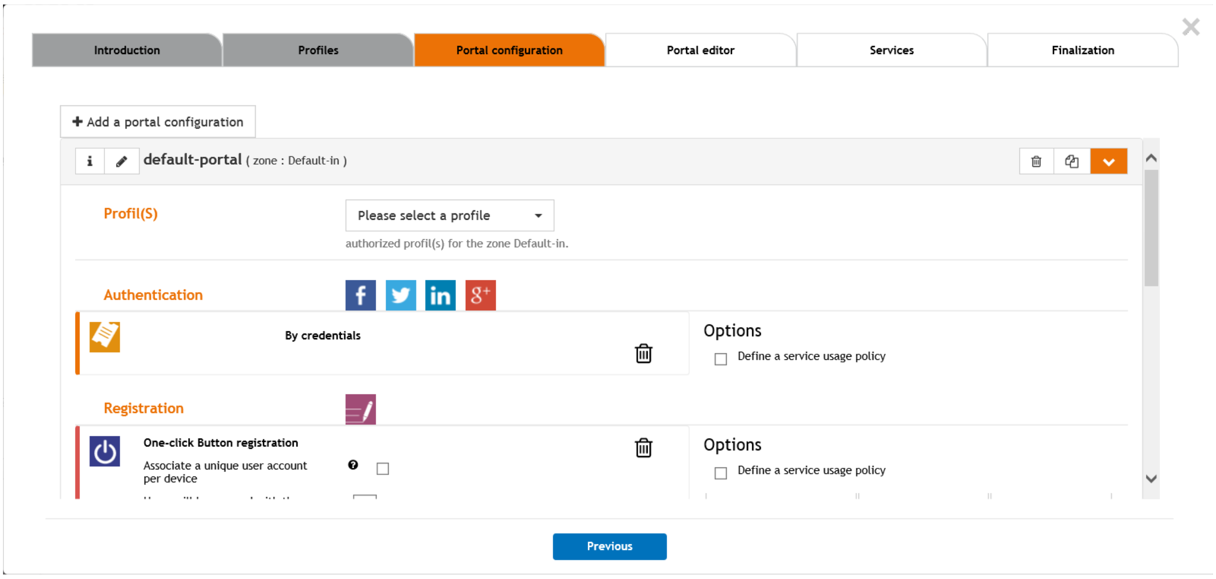
Exhibitor (Full_Access)

Previous | Next

Figure 61: Configuration wizard – Defining user profiles

2. Configuring captive portals

The authentication modes through social networks or credentials are available for configuration. The self-registration modes "One Click Button" and web form are also available.



Introduction | Profiles | Portal configuration | Portal editor | Services | Finalization

+ Add a portal configuration

default-portal (zone : Default-in)

Profil(S) Please select a profile

authorized profil(s) for the zone Default-in.

Authentication

By credentials

Options

□ Define a service usage policy

Registration

One-click Button registration

Associate a unique user account per device □

Options

□ Define a service usage policy

Previous

Figure 62: Configuration wizard – Configuring captive portals

3. Configuring visual portal

Several predefined templates portals are offered in a "responsive design" approach. These templates can be customized (background images, color, text, logo, etc.). This customization can be differentiated by type of device.

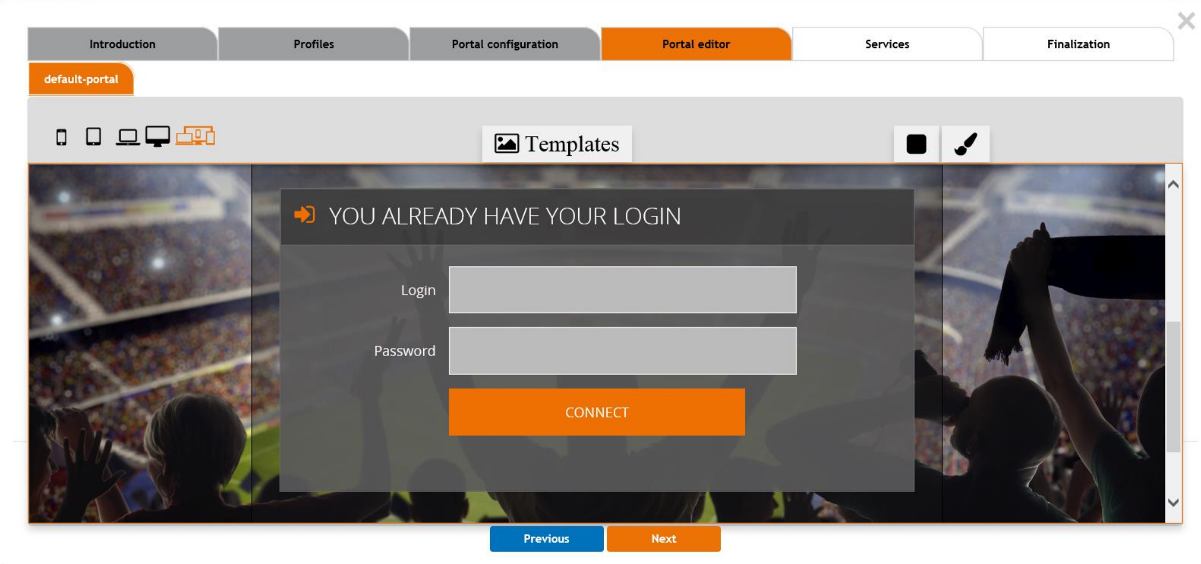


Figure 63: Configuration wizard – Configuring portal visual

4. Generating the configuration

The generated configuration can be applied on one or more controllers UCOPIA.

8.5 UWS Architecture

The UCOPIA controllers communicate with UWS through HTTPS (for statistics uploading, etc.). SSH tunnels are used for remote administration.

The architecture of UWS platform is as follows.

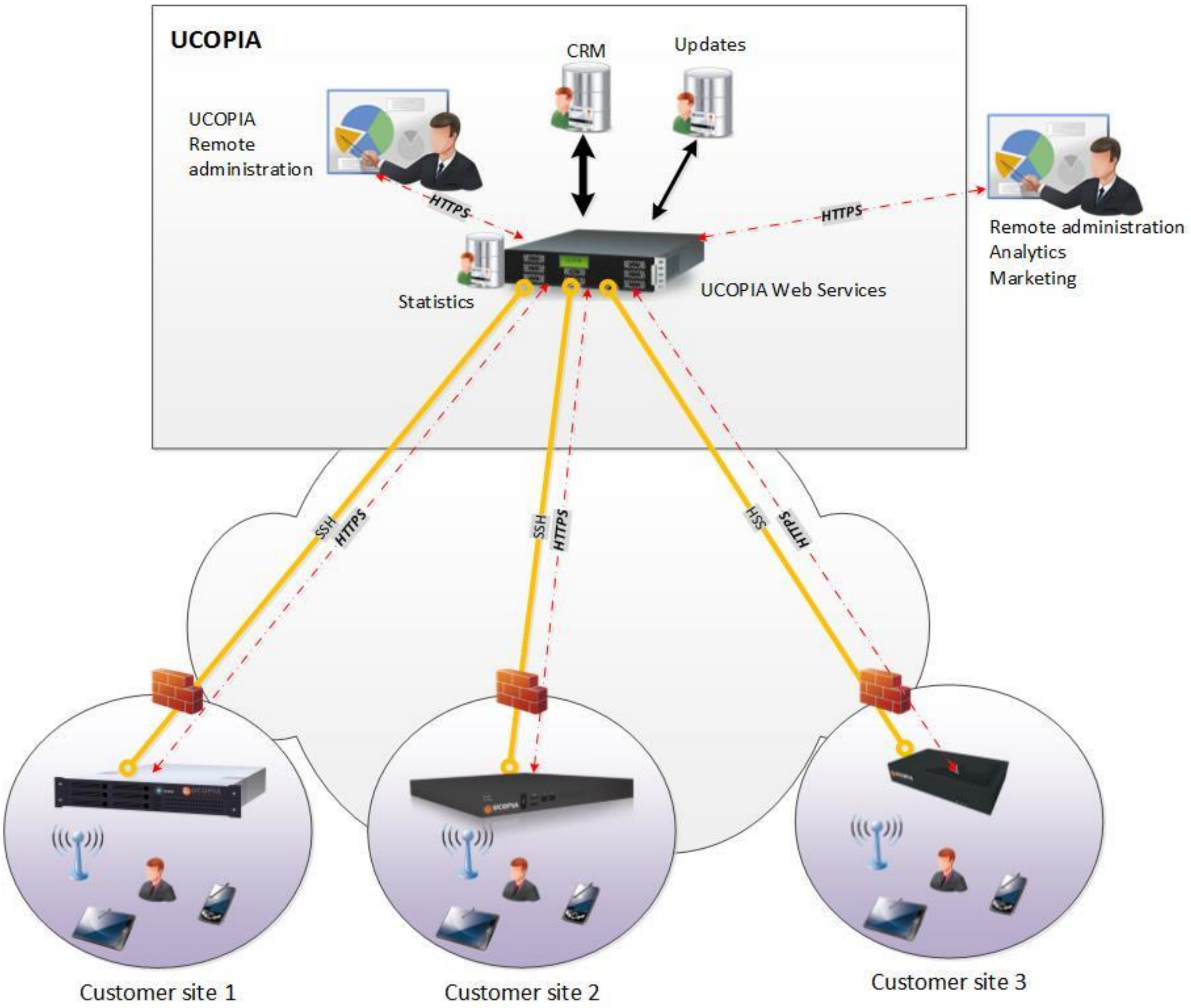


Figure 64: UWS architecture

8.6 UWS « on-premise »

Each module of the UWS platform can be offered "on-premise" for installation in the customer's infrastructure. For example, an operator can install UWS Administration “on-premise” in its datacenter to manage its pool of controllers. Another example may involve a customer who wants the Wi-Fi Marketing "on-premise" module to both have a dedicated platform for content injection and also to perform the injection locally and not in the cloud.

UWS "on-premise" modules are available as virtual appliance (VMware) or physical appliance.

9 UCOPIA product lines

UCOPIA solutions are made of one subscription service (Wi-Up) and different product lines:

- **Wi-Up service subscription** is an all-in-one service offering with a server, hardware and software maintenance, and service subscription for 3 to 5 years. The features are limited to the needs of small businesses, firms or concessions wishing to set up a service of access Wi-Fi or wired for the visitors. The Wi-Up subscription offers a simple, reliable service, in compliance with legal requirements and adapted to the needs of small structures, with a configuration fully supported via the UWS platform
- **UCOPIA Express** comes in the form of a ready-to-use appliance perfectly suited to the needs of hotels**,** hospitals**,** secondary schools and small business in general**.** UCOPIA Express provides the essential UCOPIA features in terms of security and mobility in an approach that favors the simplicity of implementation and administration**.** UCOPIA Express works without strong integration with the LAN.
- **UCOPIA Advance** offers all UCOPIA features and is designed for medium and large projects, enterprises, campus, large venues, etc. UCOPIA Advance can meet the needs of mono-site environment and offers all the functions of integration with the enterprise LAN**.** UCOPIA Advance can be redundant and also works in load balancing**.**
- **UCOPIA Advance Global** offers all the UCOPIA Advance features in a multi-site environment and is intended for medium and large projects of companies, chain stores or agencies, and multi-tenant architectures used by services providers. UCOPIA Advance Global enables you to address a significant number of remote sites with different technical architectures: centralized traffic, on premise Edge server deployment, or only on-premises Wi-Fi equipment.

The table below describes the features for each service or license:

Features	Wi-Up	Express	Advance	Advance Global OOB Edge	Advance Global OOB Vendor
Security					
Authentication					
➢ Web captive portal	●	●	●	central	central
➢ 802.1x/PEAP/TTLS		●	●		
➢ 802.1x/TLS			●		
➢ Dynamic VLAN assignment		●	●		
➢ Social networks (Facebook, Twitter, Google, LinkedIn)	● Facebook Twitter Google	●	●		Vendor dependent
➢ Customized social network apps		●	●	●	Vendor dependent
➢ OpenID Connect		●	●	●	Vendor dependent
➢ Automatic connection per subnet		●	●	●	●
➢ Automatic @MAC address authentication	●	●	●	●	●
➢ Shibboleth		●	●		
Redirection on web page before or after portal authentication		●	●	●	●
URL/domain filtering (HTTP and HTTPS)		●	●	●	●
Multiple and customizable user profiles		●	●	●	●
Controller's incoming VLANs / subnets	Native + 2 VLAN IN	●	●	●	●
Outgoing VLAN redirection on basis of user profile		●	●	●	Vendor dependent
ARP spoofing protection		●	●	●	
URLs available before authentication		●	●	●	Vendor dependent
Pre-authentication charter acceptance	●	●	●	●	●
Private information charter acceptance (opt-in marketing)		●	●	●	●

Password policies and password recovery		●	●	●	●
Quarantine after N wrong password attempts		●	●	●	●
Connection break between two sessions		●	●	●	●
Connections traceability and logs					
➤ User sessions	Handled by UCOPIA	●	●	●	●
➤ Traffic (URL, applications)	Handled by UCOPIA	●	●	●	Vendor dependent
➤ Automatic logs backup via FTP(S)	Handled by UCOPIA	●	●	●	●
➤ Automatic logs compression	Handled by UCOPIA	●	●	●	●
Audit logs (Syslog)		●	●	●	●
Mobility					
Zero configuration					
➤ DHCP/ fixed IP address	●	●	●	●	Vendor dependent
➤ Seamless mail access		●	●	●	●
➤ Seamless Internet Access (proxy)	●	●	●	●	●
➤ Seamless printer access		●	●	Per Edge	
➤ Airprint compliance		●	●	Per Edge	
QoS (by service, by user)		●	●	●	Profile mapping
Data volume quota		●	●	●	Profile mapping
Time based access control					
➤ Time slots		●	●	●	●
➤ Time credit		●	●	●	●
Location/zone based access control		●	●	●	●
Multi-portal (one portal per zone)		●	●	●	●
Conditional & adaptative profile			●	●	●
BYOD			●	●	●
UCOPIA Mobile Application	End-of-life in September 2017				
iPass compliance		●	●		

Administration					
License per zone or user profile		●	●	●	●
Security and mobility policies administration		●	●	●	●
Guest hosting and provisioning (SMS, email, form, ticket printing)		●	●	●	● No email registration autolink
Sponsoring by email			●	●	● No email registration autolink
Automatic user accounts purging (global or per profile)	Global	●	●	●	●
Manual user account exportation via CSV	●	●	●	● central	● central
Automatic user account exportation via CSV			●	● central	● central
Delegated provisioning					
➤ Customization		●	●	●	●
➤ Multi zones		●	●	●	●
➤ Connection ticket printing (or sending by SMS or email)		●	●	●	●
➤ Creating accounts in mass from a CSV file		●	●	●	●
➤ User account refill by code		●	●	●	●
Supervision of connected users	●	●	●	●	●
Statistics					
➤ Predefined graphs	●	●	●	●	●
➤ Opt-in Marketing		●	●	●	●
➤ Manual CSV export	●	●	●	●	●
➤ Automatic CVS export			●	●	●
Reporting (PDF), send by email or FTP		●	●	●	●
Customizable web portal with graphical editor	● Wizard	●	●	●	●
Customizable portal with HTML import/export		●	●	●	●
Customizable connection ticket per zone or profile		●	●	●	●

SNMP – MIB II		•	•	•	•
External Syslog		•	•	•	•
CLI	SSH CLI	•	•	•	•
Multi zone administration		•	•	•	•
Directory replication in HA			•	• central	• ` central
Physical Administration port		Hardware dependent			
Billing					
Online payment (credit card, PayPal, Ingenico)		•	•	•	•
User account refill by code or online payment		•	•	•	•
PMS connector		•	•	• central	•
PPS connector		•	•	•	•
AAA third party solutions integration (accounting)			•	•	•
Integration					
Integration with a corporate LDAP directory (OpenLDAP, ActiveDirectory)		•	•	•	•
Integration with one or more directories			•	•	•
Integration with external RADIUS (proxy)			•	•	•
Integration with secondary RADIUS (failover or load-balancing)			•	•	•
Web proxy integration		•	•	•	
ICAP compliant		•	•	•	
API for third party tool integration		•	•	•	•
Architecture					
DHCP server (IN), DHCP client (OUT)	•	•	•	•	
DNS server, relay	•	•	•	•	
NTP		•	•	•	
NAT with connection tracking (FTP, PPTP, GRE, H323, SIP, IRC, SFTP)	•	•	•	•	
Routing		•	•	•	

Customized NAT or routing based on user profile		●	●	●	
Link Aggregation Control Protocol (LACP IEEE 802.3ad)			●	●	●
High availability (Redundancy & load balancing)			●	● central	●
Wired connections	●	●	●	●	●
Remote site management with centralized, Edge or mixed architecture				●	●
Inline or out-of-band architecture	inline	inline	inline	inline & OOB	inline & OOB
Supported multisite physical location	1	1	1	Up to 2000	Up to 2000
Multi-tenant architecture				●	●
Virtual appliance (VMware and Hyper-V)		●	●	●	●
UCOPIA Web Services					
UWS Administration	●	●	●	●	● central
UWS Marketing		●	●	●	No marketing campaign based on web injection
UWS Analytics		●	●	●	●
UWS Wizard & smart configuration	●	●	●	●	●

10 Licenses

Each line of product is declined with different capacities (license), offering multiple concurrent connections.

The following table is representing the lines of products.

Express license	**Express 5**	**Express 10**	**Express 20**	**Express 50**	**Express 100**	**Express 150**	**Express 250**	**Express 500**	**Express 1000**	**Express 2000**
Number of concurrent connections	5	10	20	50	100	150	250	500	1000	2000

Advance license	**Advance 150**	**Advance 250**	**Advance 500**	**Advance 1000**	**Advance 2000**	**Advance 5000**	**Advance 10000**	**Advance 20000**

Number of concurrent connections	150	250	500	1000	2000	5000	10000	20000

Clustering with load-balancing mode can be proposed in order to reach more than 20000 concurrent users.

There is also a global license which does not apply to a particular controller but to a set of controllers. The distribution of the license on the controllers can be made via the UCOPIA Web Services platform.

11 Hardware

UCOPIA is available on four different types of hardware. All boxes include at least two 10/100/1000 Ethernet ports and hard disks for user logs backup.

The appliance **"US250"** available only with the Express range of products, allowing up to 250 concurrent users.

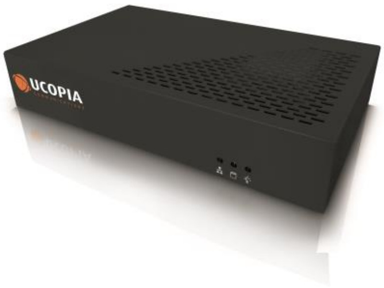


Figure 65: Appliance "US250" format

The appliance **"US2000"** used to manage up to 2000 concurrent users (Express and Advance).

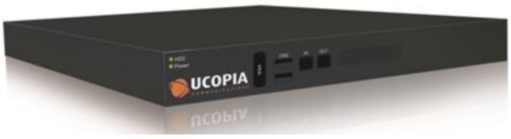


Figure 66: Appliance "US2000" format

The **"US5000RDP"** controller for solutions requiring more bandwidth and high availability. The controller is 2U format. It comprises six Ethernet ports (3 incoming, 3 outgoing) for user traffic, one Ehernet port for administration, two RAID disks and a redundant power supply.

Available only with the Advance range of products, allowing up to 5000 concurrent users.

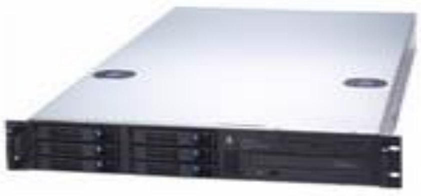


Figure 67: Appliance "US5000RDP" format

The **“US10000RDP”** controller is 2U format. It comprises height Ethernet ports (4 incoming, 4 outgoing), one Ethernet port for administration, four RAID disks and a redundant power supply.

Available only with the Advance range of products, allowing up to 10000 concurrent users.

Figure 68: Appliance “US10000RDP” format

The **“US20000RDP”** controller is 2U format. It comprises two Ethernet ports 10Gb, one Ethernet port for administration, 8 RAID disks and a redundant power supply.

Available only with the Advance range of products, allowing up to 20000 concurrent users.

Figure 69: Appliance “US20000RDP” format

The following table summarizes the different lines of products.

Express	**Express 5**	**Express 10**	**Express 20**	**Express 50**	**Express 100**	**Express 150**	**Express 250**
Hardware	US250						

Express	**Express 500**	**Express 1000**	**Express 2000**
Hardware	US2000		

Advance	Adv 150	Adv 250	Adv 500	Adva 1000	Adv 2000	Adv 5000	Adv 10000	Adv 20000
Hardware	US2000					US5000RDP	US10000RDP	US20000RDP

The following table summarizes the technical characteristics of the servers

	« US 250» Format	« US 2000 » Format	« US 5000RDP » Format	“US 10000RDP” Format	“US 20000RDP” Format
Hard drive	320 Gb	1 Tb	2 Tb (RAID 1)	4 x 900 Gb (raid 5)	8x 900 Gb (raid 6)
Network ports	2 (10/100/1000)	2 (10/100/1000)	6 (10/100/1000) 3 x IN, 3 x OUT 1 (10/100/1000) Administration	8 (10/100/1000) 4xIN, 4xOUT 1 (10/100/1000) Administration	2 x 10Gb 1 (10/100/1000) Administration
Power supply	24W	90 W	250 W (2 Hot Plug Power supply)	750 W (2 Hot Plug Power supply)	110 0W (2 Hot Plug Power supply)
Size (HxLxW)	52x270x160 mm 19’’ rack kit (optional)	44x430x500mm 19’’ 1U rack	88x430x700mm 19’’ 2U rack	88x430x700mm Rack 2U 19’’	88x430x700mm Rack 2U 19’’

All these products can be upgraded by changing the license key, if the appropriate hardware has been installed.

🔑 = software key

= hardware replacement

License	Exp. 10	Exp. 20	Exp. 50	Exp. 100	Exp. 150	Exp. 250	Exp. 500	Exp 1000	Exp 2000
Hardware	US250						US2000		
Exp.5	🔑	🔑	🔑	🔑	🔑	🔑	🖥	🖥	🖥
Exp.10		🔑	🔑	🔑	🔑	🔑	🖥	🖥	🖥
Exp.20			🔑	🔑	🔑	🔑	🖥	🖥	🖥
Exp.50				🔑	🔑	🔑	🖥	🖥	🖥
Exp. 100					🔑	🔑	🖥	🖥	🖥
Exp. 150						🔑	🖥	🖥	🖥
Exp. 250							🖥	🖥	🖥
Exp. 500								🔑	🔑
Exp 1000									🔑

License	Adv. 250	Adv. 500	Adv 1000	Adv 2000	Adv 5000	Adv 10000	Adv 20000
Hardware	US2000				US5000	US10000	US20000
Adv. 150	🔑	🔑	🔑	🔑	🖥	🖥	🖥
Adv. 250		🔑	🔑	🔑	🖥	🖥	🖥
Adv. 500			🔑	🔑	🖥	🖥	🖥
Adv 1000				🔑	🖥	🖥	🖥
Adv 2000					🖥	🖥	🖥
Adv 5000						🖥	🖥
Adv 10000							🖥

12 Virtualization

The UCOPIA solution can be delivered as a virtual appliance. The UCOPIA virtual appliance works on top of VMware and Hyper-V. Express and Advance product lines can be virtualized. All the UCOPIA features are available (redundancy and load balancing for Advance only).

Four virtual servers are available: UV250, UV2000, UV5000 and UV10000.

13 Maintenance

UCOPIA controllers are sold with a three-year maintenance contract.

The maintenance contract covers the following points:

- **Early controller replacement in the event of hardware failure. Equivalent hardware dispatched D+1 (in metropolitan France).**
- **Software patches and enhancements delivered automatically.**
- **Partner access to UCOPIA technical support service (level 2 and higher).**

14 Conclusion

UCOPIA develops and markets a solution dedicated to mobile users, enabling them to easily and safely connect to Wi-Fi or wired networks, using any type of equipment (PC, smartphone, tablet).

UCOPIA presents the following advantages and benefits.

- Professional-level security, fully compliant with legal obligations

  UCOPIA implements robust security functionalities consistent with industry standards. It provides authentication mechanisms ranging from a captive HTTPS-based portal to strong authentication based on 802.1x/EAP and RADIUS; access control based on the user, zone and time profile ; full traceability of user traffic, as well as maintaining connection logs to meet legal requirements.

  The UCOPIA solution is certified by ANSSI (the French National Agency for the Security of Information Systems) regarding its security functionalities.

- Simple and user-friendly customer experience

  UCOPIA offers a wide variety of user experience options to meet different usage needs. They include a single click action to connect to methods that require authentication and confidentiality. The recognition of user equipment enables the system to ensure a seamless connection when needed.

  The captive portal enables users to self-register and receive their credentials through various means (SMS, email, voucher, etc.).

  UCOPIA's zero-configuration mechanisms facilitate access; they enable the user to easily connect regardless of equipment or configuration.

  A mobile application for smartphones contributes to the user's comfort.

- Mobile user management

  UCOPIA enables mobile employees, clients, partners, and suppliers to connect easily and safely anywhere (mobile office, meeting or training room, etc.), in order to access their email, the Internet, and to share or print documents. There are no configuration steps or prerequisites involved for the user; they will not need to call technical support to print a document or to send a message. UCOPIA contributes to a company's branding by enabling visitors to access their network.

- An approach that can generate revenue

  The Analytics service allows a better understanding of the users and their behavior. It is then possible to offer value-added services or targeted advertising on the captive portal or on visited pages through the Web injection. This helps to promote, retain and monetize access.

  Access to services can be billed by the purchase of online packages available on the portal (credit card, PayPal, Ingenico) or through interfaces with third party billing tools.

- A high-availability solution

  With its cluster architecture, UCOPIA can ensure high availability of the service. A cluster can work in redundancy mode and/or load balancing mode.

- Optimize total cost of ownership (TCO)

  The deployment of a solution for mobile guests requires integration with the existing information system and security infrastructure. Without UCOPIA, this may require a great deal of work and time. UCOPIA integrates seamlessly with the existing network (VLAN, directory, etc.), without compromising security policies already in place. Also thanks to its ease of administration and its zero-configuration mechanisms, fewer technical resources are needed. All these benefits enable to greatly reduce the cost of ownership of such a solution.

- An evolutive and scalable solution

  UCOPIA offer comprises a wide range of products that perfectly meet the needs of small organizations providing services to a few users, as well as centralized, multi-site architectures providing thousands of simultaneous connections.

  The UCOPIA solution is managed through sophisticated, powerful tools that are user-friendly. Statistical reports (number of concurrent sessions, session duration, types of equipment used, etc.) enable to better understand how the solution is being used.

  A centralized platform allows to remotely manage and monitor a pool of UCOPIA controllers.

  The UCOPIA solution is set up independently from the network equipment and it can also operate in a heterogeneous environment, thus ensuring the sustainability of hardware choices. UCOPIA runs in wired and Wi-Fi environments; its level of abstraction from the physical network enables it to evolve together with relevant standards.

15 Appendix 1: Documentation

A documentation package is offered with the UCOPIA product.

15.1 Guides

- Installation Guide

  This guide is intended for system and/or network administrators wishing to install the UCOPIA solution. It describes the installation and configuration for all the components in the solution. There is one manual for Express and one for Advance.

- Administration Guide

  This guide is intended for system and/or network administrators responsible for managing UCOPIA.

  This guide describes the administration tool and the full set of administration procedures. There is one manual for Express and one for Advance.

- Delegated Administration Guide

  This manual describes the delegation portal. It is common to both UCOPIA product ranges: Express and Advance.

- UCOPIA Portal Editor Guide

  This manual describes the UCOPIA portal graphics editor. This manual is common to both UCOPIA product ranges: Express and Advance.

- UCOPIA User Guide

  This guide is intended for users of a network controlled by UCOPIA. It describes the use of the various portal methods.

  This manual is common to both UCOPIA product ranges: Express and Advance.

- UCOPIA CLI guide

  This guide describes the UCOPIA CLI (Command Line Interface). The interface gives access to certain network, system, or advanced administration commands.

  -

15.2 APIs

- UCOPIA delegated administration API

  The purpose of the delegated administration API is to connect the UCOPIA controller with a third party tool such as an account provisioning and/or service billing tool. The delegated administration API can be used to create, delete and modify user accounts, as well as to retrieve the cumulative connection time for a user.

- UCOPIA portal API

  - **The portal API can be used for advanced customization of the captive portal. The API defines interactions between the portal and the controller.**

15.3 Integration with third party tools

- SMS messaging via the UCOPIA controller

  UCOPIA offers an account provisioning method whereby users self-register on the UCOPIA portal using their mobile phones. They receive their connection login information by SMS.

  This document describes the various SMS platforms with which UCOPIA interfaces.

- Using UCOPIA with a PMS

  The UCOPIA controller interfaces with PMS products (Property Management System).

  This document describes how the products inter-operate.

- Using PayPal with UCOPIA

  This document describes how the UCOPIA portal works to enable users to buy packages online via PayPal. It also details how to open a PayPal account and how to configure UCOPIA accordingly.

- UCOPIA and iPass compatibility

  This document presents how UCOPIA must be configured to allow iPass user connections. Requirements regarding the network configuration are also described.

15.4 Other technical annexes

- Advanced portal customization

  This document presents how to modify the source code of the captive portal visual model for advanced customization. Useful for customization that cannot be made through the portal graphical editor (e.g.: modification of behavior).

- User log database

  Session and traffic logs are created locally on the UCOPIA box and available from the UCOPIA administration tool. The logs are stored in a SQL database.

  To facilitate integration with third party applications, UCOPIA offers connection to the SQL log database. This document describes how the database works, its entities and attributes.

- Upgrading in a High Availability environment

  This document applies to high availability architectures that have deployed the functionality of redundancy or load balancing, and have it activated. This document only covers evolutive updates toward a higher version. Corrective updates are not covered.

- Cloud architectures

  UCOPIA offers different architectures, centralized, distributed or mixed for deploying highly flexible architectures.

  This documents describes the different kinds of centralized architectures in the Cloud. For each of them we will describe the advantages and the weaknesses, the customer target and how to deploy it.

15.5 Security certification

http://www.ssi.gouv.fr/uploads/IMG/cspn/anssi-cspn_2010-01fr.pdf

16 Appendix 2: Glossary

Here is a list of key words and definition used in this document.

16.1 Network

- **DNS - Domain Name Service**: Domain name service, allowing to associate a domain name to an IP address.
- **SNMP - Simple (or Smart) Network Management Protocol**: Protocol belonging to the application layer of the OSI model, used for network administration.
- **HTTPS - Hyper Text Transfer Protocol over SSL:** Transmission protocol offering a secure connection between a client and a server using sockets.
- **VLAN – Virtual Local Area Network**: Allowing realizing multiple logical networks on the same physical link.
- **DHCP – Dynamic Host Configuration Protocol:** Protocol providing IP addresses to a device connecting on a network.
- **NAT – Network Address Translation:** Mechanism allowing translating multiple private IP addresses to one public IP address.
- **ICAP – Internet Content Adaptation Protocol : The ICAP protocol is a lightweight HTTP like protocol which is used to extend transparent proxy servers, thereby freeing up resources and standardizing the way in which new features are implemented. ICAP is generally used to implement virus scanning and content filtering in transparent HTTP proxy caches.**

16.2 Wi-Fi

- **Wi-Fi – Wireless Fidelity**: Wi-Fi is a commercial brand promoted by the Wi-Fi Alliance, an industry consortium of manufacturers and vendors. The Alliance certifies the compliance of products to IEEE standards (802.11 family).
- **802.11 b/a/g/n:** 802.11 is a set of standards defined by IEEE. The letters b, a, g, n identify different throughputs and underlying protocols (from 10 to 500 Mbps). 802.11n offers bandwidth in excess of 100 Mbps.
- **802.11i:** Security standard for WI-Fi ratified in June 2004. It includes 802.1x for strong authentication and AES encryption. 802.11i requires new equipments both on the AP and the client side.
- **802.11e:** Standard for Quality of Service. It is not ratified. 802.11e aims to give possibilities in terms of quality of service at the level of the data link layer. The purpose of this standard is consequently to define the requirements for the various packets in terms of bandwidth and transmission time in such a way as to enable improved voice and video transmission in particular.
- **802.11f:** Standard for roaming. It is not ratified. 802.11f is a recommendation for access point vendors for improved product interoperability. It offers the Inter-Access Point Roaming Protocol enabling a roaming user to transparently change access point while on the move, regardless of the access point brands found on the network infrastructure.

16.3 Authentication

- **802.1x:** Hardware-independent network access control standard. The network allows only authentication traffic through until authentication is successfully completed. 802.1x also specifies the EAPOL (EAP over LAN) protocol, which enables EAP authentication methods to be encapsulated.
- **EAP – Extensible Authentication Protocol:** EAP is a protocol to transport authentication data. This protocol operates at OSI level 2, before the client has an IP address to enforce security. EAP works for both wired and wireless networks. Based on EAP, many authentication solutions can be implemented, based on password (PEAP, TTLS), certificates (TLS) and more. A RADIUS server is used to drive the dialogue with the client. 802.1x is the name of EAP applied to 802.11 networks.
- **EAP-MD5:** The client is authenticated by the server using a challenge-response mechanism. The server sends a random value (the challenge). The client concatenates the password to the challenge and calculates, using the MD5 algorithm, a "hash" that it returns to the server. The server, which knows the password, calculates its own hash, compares the two and either approves or rejects authentication depending on the result.
- **LEAP – Lightweight EAP:** is a proprietary Cisco method based on the use of shared secrets for mutual server and client authentication. It does not use a certificate and is based on exchanging a challenge and response.
- **EAP-TTLS – Tunneled Transport Layer Security:** uses TLS as a tunnel to exchange attribute-value pairs in the same way as RADIUS when used for authentication.
- **PEAP – Protected EAP:** is a method that has very similar objectives and works in a similar way to EAP-TTLS. It was developed by Microsoft. It uses a TLS tunnel to transport EAP. It is then possible to use all authentication methods supported by EAP.
- **EAP-TLS – Extensible Authentication Protocol-Transport Layer Security:** This is the safest. The server and client each have a certificate which will be used for mutual authentication. It remains relatively restricting, owing to the need to deploy a key management infrastructure. It should be recalled that TLS, the standardised version of SSL (Secure Socket Layer) transports messages securely (encryption, mutual authentication, integrity checks).
- **NTLM – NT LAN Manager:** is a Microsoft authentication protocol. This protocol uses a challenge-response mechanism for authentication within which client can prove their identity without sending a password to the server. The protocol consists of three messages: Type 1 (negotiation), Type 2 (challenge) and Type 3 (authentication).
- **PKI – Public Key Infrastructure:** PKI is an architecture based on public and private keys stored in certificates. This enables organizations to deploy secure solution to exchange emails, documents with the guarantee of confidentiality. With PKI, A can send an email to B, be sure that only B will read, and prove that only A could send it. PKI can be used to mutually authenticate on a network. This is done through a standard architecture called EAP/TLS. UCOPIA enables customers PKI already in place to be used for Wi-Fi authentication.
- **RADIUS - Remote Access Dial-in User Services:** RADIUS is a standard protocol to query remotely an authentication server. UCOPIA includes a RADIUS server.
- **OTP - One Time Password:** One time password solutions generate a password which is limited in time. This enhances security. The most famous and spread OTP solution is RSA secure ID. UCOPIA enables organizations which already deployed OTP to use them to authenticate on a Wi-Fi network.
- **SSO – Single Sign On:** SSO is used to unify authentication procedures. Single Sign-On makes it possible to combine all authentication requests into one procedure. This improves both the user experience and the security level.

- **WISPr – Wireless Internet Service Provider roaming :** pronounced "whisper", WISPr is a protocol submitted to the Wi-Fi Alliance that allows users to roam between wireless internet service providers, in a fashion similar to that used to allow cellphone users to roam between carriers. A RADIUS server is used to authenticate the subscriber's credentials.

16.4 Encryption

- **WEP - Wired Equivalent Protection:** WEP is an encryption algorithm based on 64 bits keys, used in first generation Wi-Fi access points. WEP is known as very weak because keys are small, static and shared by several users.
- **TKIP – Temporary Key Interchange Protocol:** With TKIP, encryption keys are created dynamically and changed periodically. This addresses the major WEP weaknesses. TKIP is upward compatible with WEP APs.
- **AES, DES, 3DES:** These are encryption algorithm using 128 bits keys. They are used in VPN solutions and for encryption in latest generation APs.
- **VPN – Virtual Private Network:** VPN enables to build a virtual private network on top of a shared, public physical infrastructure. VPNs implement authentication and encryption technologies to deliver for instance secure remote access to corporate information systems.
- **IPSec:** This is a particular VPN technology that operates at level 3 of the network. Any application can seamlessly rely on a VPN. IPSec requires a client and server architecture.
- **SSL (Secure Socket Layer) and HTTPS:** SSL is an Internet standard VPN technology. Internet browsers integrate SSL. Therefore, there is no need to deploy a client to use an SSL VPN. However, SSL only apply to Internet applications. It does not apply for traditional client/server applications.
- **WPA – Wireless Protected Access:** WPA is a set of standard to enhance wireless network security. It includes 802.1x and TKIP. Main benefit compared to 802.11I is upward compatibility for existing APs and cards.
- **WPA2 :** Reinforces WPA security by making use of the AES encryption algorithm.
- **WPA-PSK - Pre Shared Key:** This method allows WPA security to be used without having an authentication server. The WPA-PSK configuration starts by determining a static key or passphrase, as for WEP. However, using TKIP, WPA-PSK automatically changes keys after a preset time interval.
- **DPSK – Dynamic Pre Share Key :** Ruckus solution that allows to deliver dynamically an unique encryption key per user.

16.5 Directory

- **LDAP – Light Directory Access Protocol:** LDAP is a standard protocol to query and update a directory across a network. Whether the directory is implemented as a file, a database or a native LDAP structure does not matter.
- **LDAPS – LDAP over SSL:** Secured protocol to query an LDAP directory.

UCOPIA

TURN YOUR WI-FI UP

www.ucopia.com