UCOPIA
COMMUNICATIONS

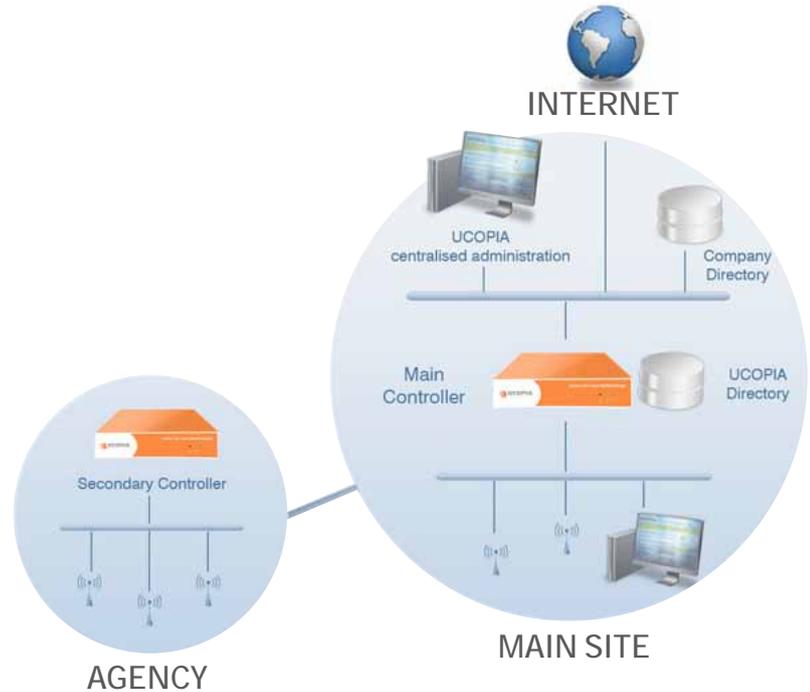## THE UCOPIA ADVANCE SOLUTION

Facilitate a productive environment for your contractors, partners and visitors with guest internet access on your premises.
UCOPIA Advance targets medium-sized and large organisations, for multiple locations deployments, access to critical applications and services, and completes integration with legacy infrastructure.

ADVANCE 100
> 100 concurrent connections

ADVANCE 200
> 200 concurrent connections

ADVANCE 300
> 300 concurrent connections

ADVANCE 500
> 500 concurrent connections

ADVANCE 1000
> 1000 concurrent connections

ADVANCE 1000 RDP
> 1000 concurrent connections

INTERNET

MAIN SITE

AGENCY

UCOPIA Advance is positionned between a corporate LAN and a wired (Ethernet, DSLAM, CPL) or wireless (Wi-Fi) access network.
All traffic to or from users pass through the UCOPIA Advance controller to ensure security, simplify LAN integration, help along administration and improve user experience. Depending on the model, UCOPIA Advance is able to handle up to 1 000 concurrent users.
UCOPIA Advance is very easy to set up and operate
thanks to its high level, user-friendly graphical administration interface.
UCOPIA Advance is used for centralised administration and provides adaptable multi-portal, multi-zone and multi-profile options.
UCOPIA Advance also offers redundancy and load-balancing mechanisms.

✕ IN-HOUSE SECURITY

UCOPIA Advance offers a full, robust security solution built on industry standards for data access and routing, on wired and wireless networks.

USER AUTHENTICATION

UCOPIA Advance allows various authentication mechanisms based on 802.1x (PEAP, TTLS, TLS) or HTTPS protocols to be implemented.

UCOPIA Advance has an embedded RADIUS server and is able to use one or more LDAP or Active Directory corporate directories to carry out authentication. In addition, UCOPIA Advance offers advanced authentication mechanisms such as cascading directories, a RADIUS proxy, authentication by zone, etc.

Administration of authentication policies for the various user populations is carried out very simply via a secure Web interface.
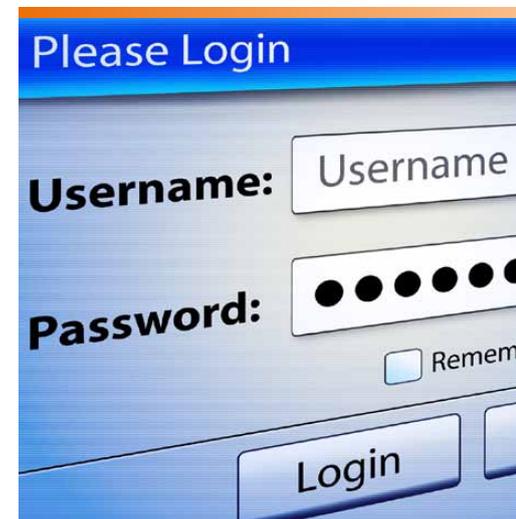
STRICT MANAGEMENT OF ACCESS RIGHTS

Each user has a profile, describing precisely that user's access rights (internet, email, in-house applications) depending on time, location and user role in the organization. Profiles are dynamically applied whenever users are logged in.

Depending on the user's profile, UCOPIA Advance may check which VLANs are authorised as inputs to and outputs from the controller.

DATA CONFIDENTIALITY

UCOPIA Advance complies with the encryption standards available in the terminals (TKIP, AES) and standardised by the IEEE 802.11i.

UCOPIA also confines different users groups on different VLANs to enhance data and user protection.

CONNECTION DATA LOGGING

Whenever an organisation delivers network access to visitors, it is legally obliged to retain from 6 to 24 months the connection data of those visitors who connect to the network (European directive 2006-24-EC and the French decree of 24 March 2006).

UCOPIA Advance meets this requirement by managing session logs (who connected when) and activity logs (who did what). This data is stored in a dedicated SQL database and it can also be used to optimise the network.

UCOPIA Advance is a solution that is independent of the Wi-Fi equipments and that will flexibly adapt to any changes that may occur in network architecture and hardware.

UCOPIA thus runs in a disparate environment (access points from different manufacturers).

UCOPIA Advance offers redundancy and load-balancing mechanisms involving two or more UCOPIA Advance controllers. This ensures the solution's availability in the event of a controller failure; furthermore the load balancing between controllers is a flexible response to the needs of increasing workloads.

⋌ MOBILITY MANAGEMENT

GUEST ACCESS

UCOPIA Advance offers a straightforward and user-friendly Web tool enabling visitors to use the network. Using this tool, an authorised individual will be able to create a temporary account, and select a predefined profile with a time slot and/or time credit.

A connection ticket will be generated and handed to the user. In addition to this visitor hosting tool, UCOPIA offers solutions allowing users to self-register on the UCOPIA portal. Under these circumstances, no third party intervention is necessary; users receive their connection settings via text message or by email or buy time credit on-line making payment by credit card.

ZERO CONFIGURATION MOBILE ACCESS

User workstations (PCs or PDAs) are not always configured appropriately for connecting to the access network.

UCOPIA Advance allows users to connect and access network resources with no prior workstation configuration or installation, and with no need for technical support. IP addressing, internet proxies, email, printing, etc. are all handled automatically.

User experience is greatly increased and technical support work reduced to a minimum.

MULTI-SITE DEPLOYMENT

In a multi-site environment, mobile users need to be given a profile suitable for the connection environment. UCOPIA Advance allows automatic adaptation of the profile depending on various criteria the place where the connection is from (site, zone), the time of connexion, or even criterious the Advance controller the user is connected to.

STRAIGHTFORWARD AND CENTRALISED ADMINISTRATION

UCOPIA Advance offers a set of solutions allowing various centralised or distributed architectures to be implemented. A multi-controller UCOPIA architecture can be deployed either to cope with increased workload, or as part of a multi-site architecture.

In all these architectures, administration of all the UCOPIA Advance controllers deployed can be centralised from one main UCOPIA Advance controller (configuration, supervision).

✕ EVOLUTION

UCOPIA Advance is a solution that is independent of the Wi-Fi equipments and that will flexibly adapt to any changes that may occur in network architecture and hardware.
UCOPIA thus runs in a disparate environment (access points from different manufacturers).

✕ HIGH AVAILABILITY

UCOPIA Advance offers redundancy and load-balancing mechanisms involving two or more UCOPIA Advance controllers. This ensures the solution's availability in the event of a controller failure; furthermore the load balancing between controllers is a flexible response to the needs of increasing workloads.

✕ UCOPIA ADVANCE BENEFITS

- Simplified Guest Account Provisioning
- Usage and Audit Data
- Business security
- A redundancy and a load-balancing mechanisms
- Branding and Web pages customization
- Online payment & integration with third party software (eg PMS)
- Mobile devices (smart phone, tablets) applications
- Seamless provisioning
- Zero configuration

THE ADVANCE SOLUTION IN BRIEF

Appliance	Advance 100	Advance 200	Advance 300	Advance 500	Advance 1000	Advance 1000 RDP
Capacity (concurrents connections)	100	200	300	500	1000	1000
Hardware (minimum request)	Server 500 (Rack1U)				Server 1000 (Rack1U)	Server 1000 (Rack2U)

FEATURES

Security	• Authentication (Captive web portal ; 802.1x/PEAP ; 802.1x/TTLS ; 802.1x/TLS ; Windows domain ; MAC Adress or IP address) • URLs accessible pre-authentication • Periodic transparent authentication (portal mode) • • Policy acceptance pre-authentication • Redirection to corporate portal	• Credit card online payment via Paypal or Payline • Access rights varying with user profile • Intusions detection • 802.11i compliant • Redirection to outgoing VLAN depending on user profile • Controller's incoming VLANs
Mobility	• Zero configuration (DHCP/fixed IP mode ; Transparent email access ; Transparent internet access ; Transparent printer access) • Adaptable profiles • VPN pass through	• QoS • Connection time slot • Time credit • Location by input and output zone • Multi-portal
Administration	• Security and mobility policy administration (services, user profiles, etc.) • Account provisioning using a text message or email • Delegated administration (visitor zone) • Bulk account creation from a CSV file • Portal and connection ticket editor • Centralised multi-controller administration	• SNMP • Supervision of connected users • Statistics • Traceability (User session logging ; User traffic logging (URL, applications) ; Automatic backup of log files via FTP) • Issuing connection tickets
Intégration	• Integration with a corporate LDAP directory (OpenLDAP, ActiveDirectory) • Integration with more than one directory • Directory cascading • Integration with RADIUS (proxy) • Integration with Web proxy	• Incoming VLAN integration • Outgoing VLAN integration • PKI integration • Third party product API integration • Prepayed System connector (prepayed Cards) • PMS connector
Archi-tecture	• DHCP server • Redundancy • NAT • Routing	• NAT or routing depending on user profile • Multi site (multi controller) • Load balancing • Wired connection of user workstations

	POWER SUPPLY	DIMENSIONS H x W x L
Server 500 (Rack)	80 W	44 x 430 x 470
Server 1000 (Rack)	90W	44 x 430 x 505
Server 1000 RDP	250 W	88 x 430 x 700