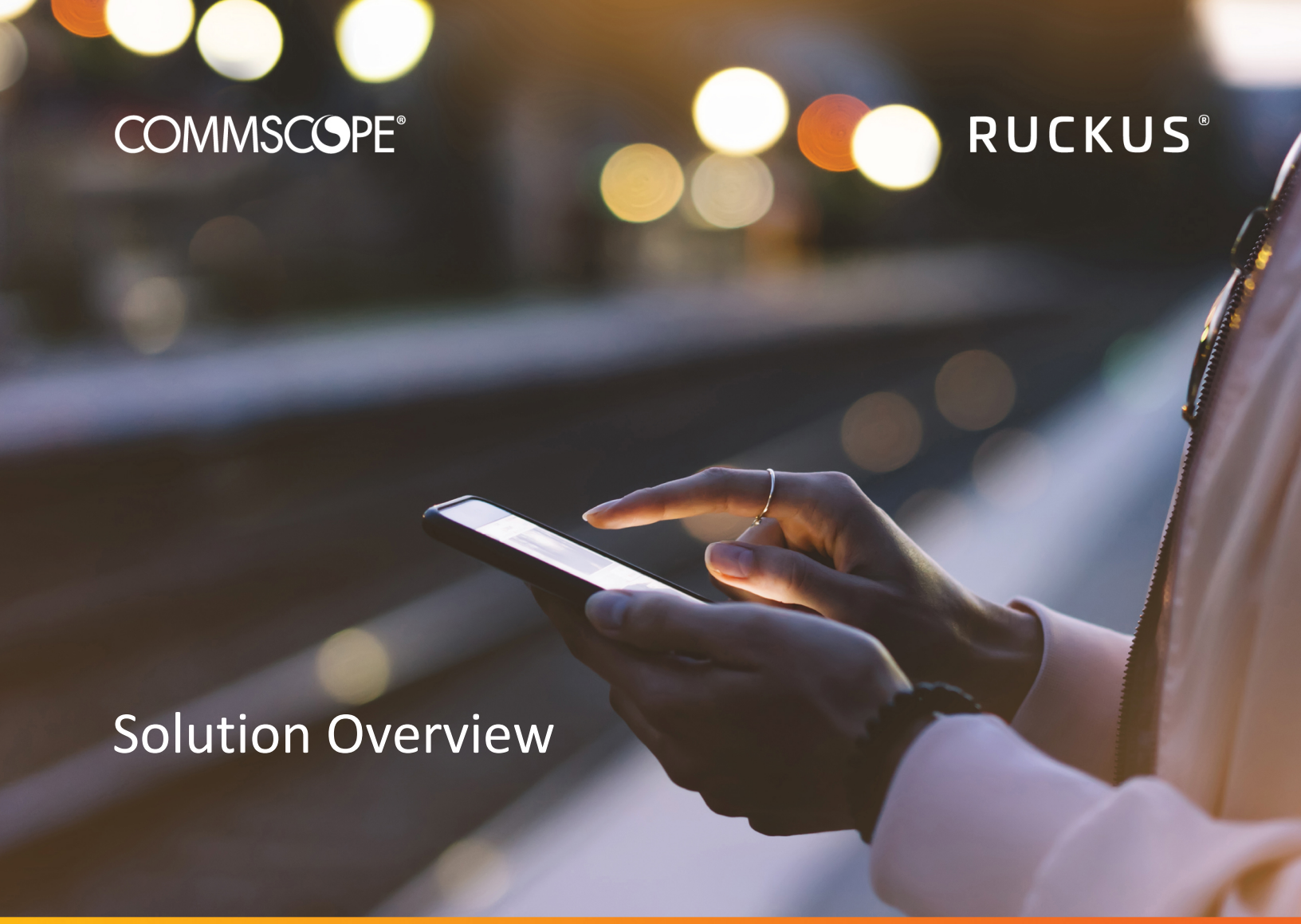

Solution Overview

RUCKUS & Mobimesh Solution Overview
August 2021

Table of Contents

5

Introduction

MobiMESH inPiazza is a complete authentication system capable of authenticating and keeping track of users connected to the system, it also enables a set of value-added services.

The system is a complete and open platform, oriented to geographical applications with large numbers of users and equipped with connectors to interface with other networks in order to allow the creation of a network federation on a municipal scale and integration with Roaming Partner.

MobiMESH inPiazza is easy to customize and to adapt to the needs of the Customer. It has numerous connectors to allow interfacing with external systems (RADIUS server, IDP / SP architectures, etc.); it is also easily customizable thanks to the support of our development team.

The system is marketed with an approach that distinguishes the hardware component from the software one; it is possible to purchase the various components of the platform in software version to install them on machine owned by the user, sized according to MobiMESH specifications or it is possible to install them in a suitably sized and configured virtualized Datacenter environment.

Alternatively, you can also purchase hardware appliances, effectively acquiring complete hardware and software appliances.

The software component follows a licensing approach, whereby the various components and features are activated individually, in order to guarantee greater flexibility and adherence to customer needs and better scalability.

The MobiMESH inPiazza is a product developed by MobiMESH and is widely referenced throughout the national territory with installations at municipal/public administration and private level.

Architecture description

The logical architecture of the MobiMESH inPiazza is composed of:

- **Captive Portal**

  it is the macro component managing the authentication process, in turn including the following elements:
- **AAA**: the *Authentication Authorization* and *Accounting* server, which ensures the tracking of sessions, the maintenance of information on local accounts, the validation of credentials and the management of policies.
- **DB**: the database that contains user data, session logs and system configuration information.
- **WP**: also known as the *Welcome Page*, the entry point to the system which includes all login methods and information displayed to the end user in a website that is easy to customize;

  Gateway or NAS

  this is the component that intercepts unauthenticated user traffic redirecting it to the Welcome Page; it is a component that is therefore always "traversed" by client data and employs the greatest amount of necessary processing.
- **Location & Business Analytics**

  this component gathers data from several data sources, to provide Analytics and insights regarding the end user's behaviour. Data are gathered from the Captive Portal module (for ex. number of logins, type of logins, returns, dwell time, etc.), from the Wi-Fi Probing component (number of devices in the area, device type, device OS, etc.) and from other Location infrastructures (Video Analytics, Bluetooth, or UWB-based location systems, etc.). Such information are managed by the A.I. engine and shown through Analytics dashboards, which are oriented to take Business decisions.
- **Recontact Module**

  this module is designed to automatically re-contact users that enter the User DB upon events that may be connected to their activity on the physical venue. The User DB is fed by the Captive Portal registrations (i.e., users that subscribe to access the Wi-Fi network and that give consent to be digitally re-contacted), but also from third-party databases. The Recontact module allows the definition of Recontact campaigns that can be operated by email, SMS, etc., and that depend on the "history" of the user behavior. For example, a survey email can be sent when the user leaves the venue (and the Wi-Fi network), or an SMS suggesting to leave a review can be sent to the user 3 days after the end of the last visit to the venue.

NAS are divided into two broad categories:

- **MobiMESH Gateway**

  brand agnostic this is the solution valid for all wireless devices (and all IP access technologies), in the form of an appliance or software to be installed on a VM in the field, it takes care of the functionality of a NAS, decoupling the login component from the authentication component. Any managed or unmanaged access point can be connected upstream of a MobiMESH NAS in order to transform it into a Wi-Fi hotspot. In this configuration, the APs only act as an intermediary from the wireless to the wired world by forwarding all the received packets. All the logic is implemented by the gateway which in turn will allow the packets of authenticated users to access the Internet and redirect those not yet authenticated to WP and AAA.
- **Smart Access Points**

  the APs of the brands supported by the platform can be configured to be used as NAS, thus redirecting to the Welcome Page, and communicating with the Authenticator for AAA functions. In this case, there is no need for a field gateway, but the platform capabilities are limited by the features supported by each NAS, which differ from brand to brand. The brands supported by the platform are considerable in number, among them CommScope/Ruckus access points stand out.

Centralized architecture

This architecture unifies in a single point the Welcome Page, Authenticator (and the related DB) plus the NAS component; it is therefore the typical configuration of scenarios in which Internet access is available through a single point (hereinafter referred to as NOC for simplicity). All user traffic is conveyed through this point before accessing the Internet. In the centralized configuration, since it is already necessary to install the Authenticator in the customer's network, it is common to activate the NAS component on the Captive Portal, thus creating a simple, effective all-in-one solution that reduces the installation and maintenance costs.

The typical conformation of this type of architecture is shown in the following figure: a set of terminals to which public access to the Internet must be guaranteed are connected to a WLAN/LAN network downstream of which the Captive Portal is located.

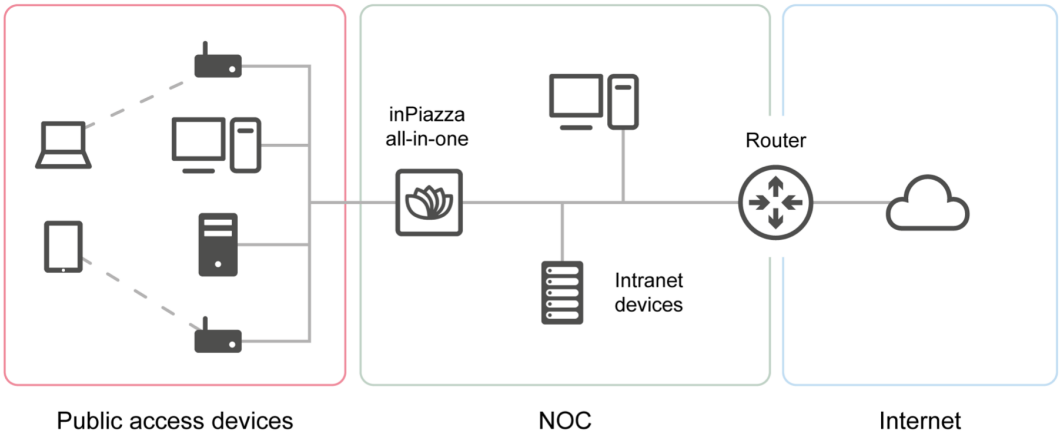

FIGURE 1: THE CAPTIVE PORTAL AS A SINGLE FUNCTIONAL BLOCK.

It is important to note that end users can access the network using a wireless or wired connection; the Captive Portal architecture is in fact independent of the technology used and therefore does not present limitations with respect to integration with heterogeneous networks, different brands or technologies.

The connection between the access equipment (Access Point, LAN points, etc.) and the Captive Portal can be of any type and technology, thus including layer 2 or layer 3 networks; this model is therefore applicable even if the APs are physically distributed in different locations connected by a single Intranet (LAN, MAN or WAN). The sole requirement in this scenario is that the user traffic must cross the all-in-one Captive Portal machine or the CP Gateway.

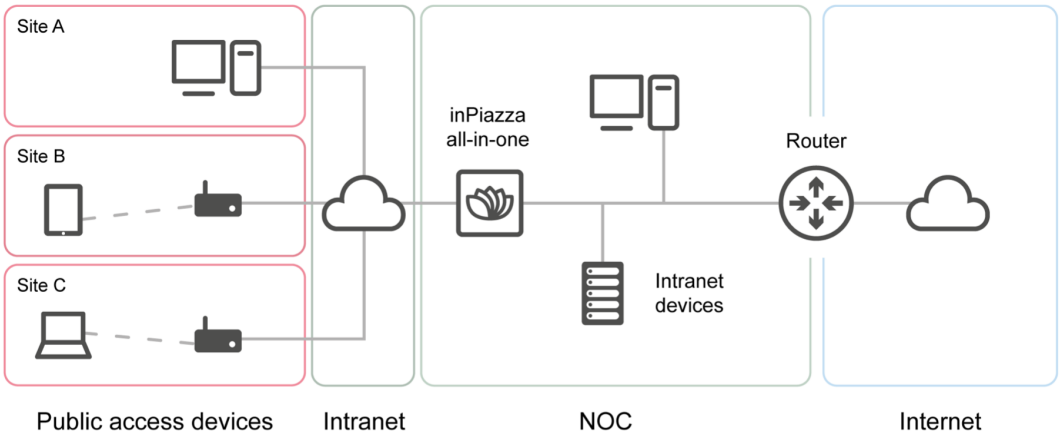

FIGURE 2: CENTRALIZED ARCHITECTURE WITH A MULTI-SITE CONFIGURATION

Distributed architecture

Distributed architecture is applied in scenarios where there are multiple offices or access areas, each of which has its own connectivity and there is no Intranet interconnecting them. The centralized architecture paradigm is also applicable in this type of scenario but tunnels and or VPNs are needed. Creating ad-hoc tunnels from remote areas to the NOC and maintaining the Captive Portal architecture solely at the NOC come at the price of wasting a significant amount of bandwidth, since all user traffic would have to be sent over the WAN to the NOC, and then back out on the Internet. This type of solution is not efficient so for this type of scenario we generally opt for a distributed approach.

The distributed approach involves the use of separate components of the Captive Portal for remote sites and for the NOC, in particular:

- the Captive Portal Authenticator (with its DB and the Welcome Page) is positioned at the NOC, it is important to make the Captive Portal Authenticator reachable by the clients accessing the Welcome Page from the various remote sites;

- a Captive Portal Gateway is positioned at each remote site, placed between the access component (AP, switch, etc.) and the local Internet access.

-

- In this configuration, the user traffic, once authenticated, is conveyed directly to the Internet through the individual local connections, and only authentication is performed within the NOC. The operational flow is therefore as follows:

- the user at the remote site starts browsing the Internet and is intercepted by the local gateway, which redirects him to the remote Welcome Page, where the user enters his credentials.
- those credentials are sent using a web method (usually a POST on a HTTPS endpoint) performed directly on the gateway.
- the local gateway contacts the Authenticator at the NOC and verifies those credentials (using an appropriate protocol: e.g., RADIUS); if these are positively verified (valid user account, valid permissions, guaranteed bandwidth, etc.), the gateway removes all the limitations and allows the user to surf the Internet through local Internet access;
- the Authenticator keeps track of the session start, and then tracks the end in a similar way when clients terminate their connection or when they exhaust their rights to navigate (e.g., session time, total GB, etc).

With this logic, a considerable saving of bandwidth is obtained at the NOC, which does not necessarily need a symmetrical bandwidth to accept user connections from remote sites.

It is possible to use the distributed and centralized approach in a mixed way into the same network, depending on the opportunity; Some sites, interconnected through Intranet, can be centralized using a gateway placed inside the NOC, while other remote sites can be managed with the distributed approach, implementing a hybrid model that can manage any possible scenario.

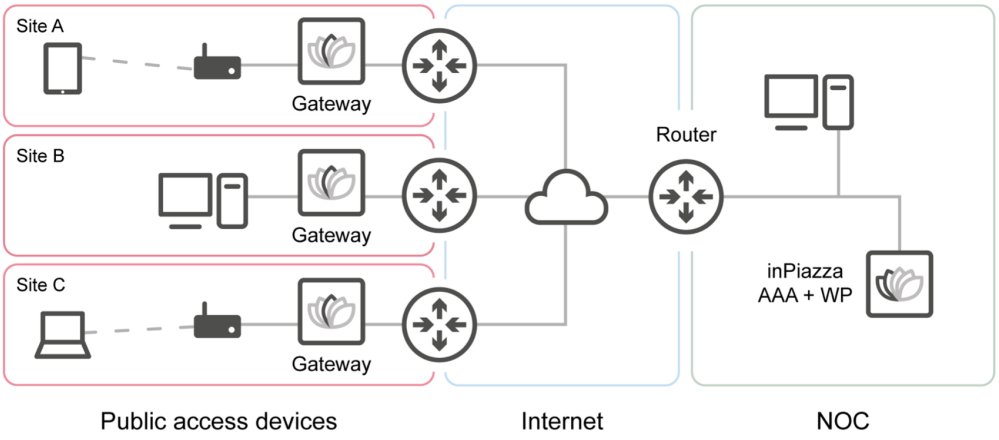

FIGURE 3: DISTRIBUTED ARCHITECTURE

Sparse distributed architecture

The sparse distributed architecture is a sub-category of the previous one. Similar to its parent, it is to be applied in scenarios where there are multiple access areas, each of them equipped with its own connectivity and furnished with a smart wireless infrastructure governed by a controller (e.g., Ruckus SmartZone).

The sparse distributed approach involves the use of the sole Captive Portal Authenticator (with its DB and the Welcome Page), while delegating the gateway part to the smart wireless infrastructure. The components are separated as follows:

- the Captive Portal Authenticator (with its DB and the Welcome Page) is positioned in a datacenter (or at the NOC) and it must be reachable by the accessing clients.
- in another datacenter (maybe the same or at the NOC) is activated the smart access point controller (i.e., the Ruckus SmartZone);
- smart APs are installed at each remote site, pointing to the controller, and propagating a particular wireless SSID: the guest WiFi network with hotspot authentication mechanism.

In this configuration, user traffic is blocked directly by the access point, then it will be redirected to the Welcome Page and only after the AP and/or controller have verified the status of the authentication with the Captive Portal, the traffic will be allowed to go towards the Internet. The consistency and the update of session data

(duration, data exchanged, location, etc.) is maintained between the access point, controller and Captive Portal through the exchange of RADIUS accounting messages.

With this architectural logic, in addition to obtaining a considerable bandwidth saving (as for the distributed solution), there is also the advantage of being able to manage a greater number of offices or areas (i.e. better scalability), of being able to configure more wireless devices at the same time and make WiFi hotspot networks coexist with other corporate networks by separating traffic at the AP level. Finally, there is also a saving on the number of devices installed since it is no longer necessary to have a gateway positioned in each access area.

It is possible to make both smart AP and Captive Portal Gateway coexist in the same network with a sparse distributed approach to meet the most heterogeneous needs (e.g., multiple locations, some with smart APs and others with basic wireless infrastructure).

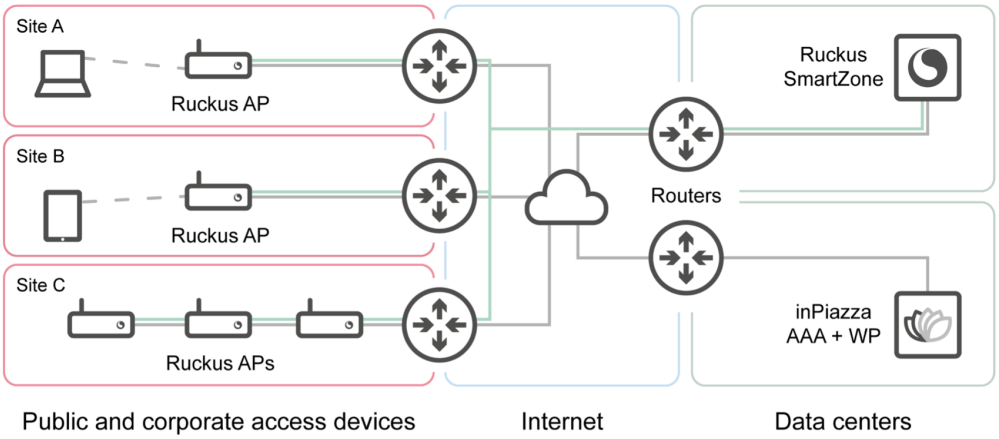

FIGURE 4: SPARSE DISTRIBUTED ARCHITECTURE

Behavior of the Mobimesh Captive Portal system

The MobiMESH Captive Portal is a user authentication system for accessing network resources; the system intercepts the connections of the users to the network and, if they are made by a not authenticated user, redirects users to the authentication page, where it is possible to provide their access credentials, which, if positively verified, will guarantee the user to proceed with access to the Internet.

Operations list:

- intercept the connections of users who want to access the network.
- redirect the user to a Welcome Page (WP) on which there is a set of initial welcome information and the forms necessary to register for the service and to authenticate.
- allows the self-registration of users, with the association of credentials to a cellular network number or with the possibility of obtaining them through an operator.
- allows users with valid credentials to access the Internet in the manner specified by the tickets assigned to them.
- allows unlimited navigation on the sites included in a list, called Walled Garden, which can be enabled and modified by the network operator.
- allows the network operator to determine which protocols (TCP/IP) to allow registered users before and after authentication.
- allows the network operator to determine the types of tickets, which define the ability of users to access the Internet, which can be delivered on the network; tickets can be defined by imposing constraints on navigation time, on cadenced repetitions (eg: 1 hour per day), on the amount of traffic, etc.:
- allows the user to acquire tickets via scratch card, group code or other methods.

Welcome Page

The Welcome Page is the page that is presented to the user who connects to the network, and it is used to register or authenticate to the service, to obtain useful information to access the Internet. The Welcome Page can be customized directly by the Customer through a simple web interface that allows you to modify the graphics and contents of the page itself.

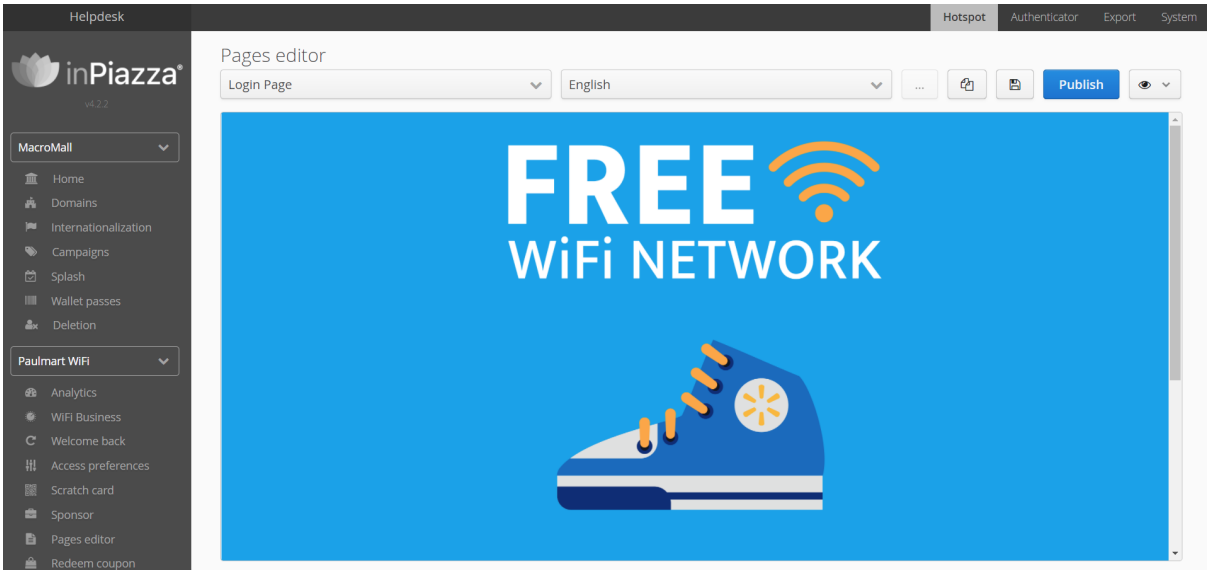

FIGURE 5: WELCOME PAGE

Each section of the Welcome Page can be customized by inserting images, texts, HTML, etc. at the appropriate points, through the point and click web editor.

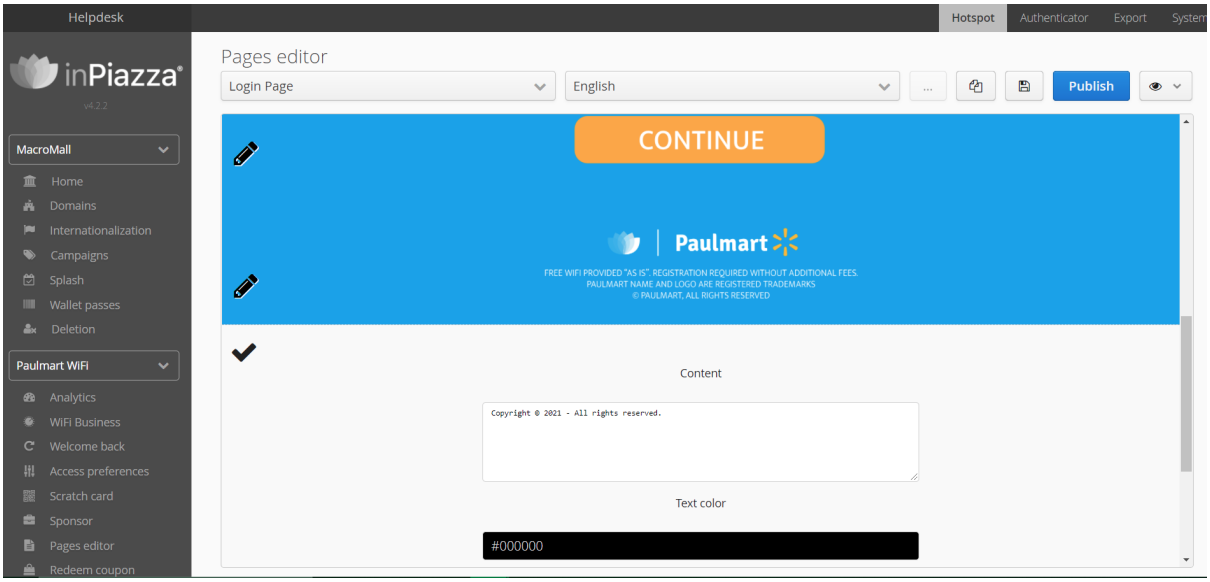

FIGURE 6: WELCOME PAGE 2

The Welcome Page also shows the authentication and registration methods selected by the user (see the relevant section below), so it is responsive, and automatically adapts to the various formats and sizes of the devices.

The Welcome Page is one of the components of the Service Profile; in fact, each Service Profile provides authentication methods, access policies and the Welcome Page, and can be applied to a single location or to a set of locations, so it is possible to provide a different Welcome Page for each Customer office, or for each set of Customer offices.

Authentication methods

- **Classic login**

  authentication by username and password, verified on the local database of the system;
- **User & password via SMS**

  registering the user via SMS and authenticating with the credentials sent by SMS. This mode, thanks to sending credentials via SMS, guarantees the unique association of the account to the phone number, and therefore the identification.
- **Hangup call**

  similar to the previous one, users must authenticate with username (phone number) and password. The phone number provided must be verified by calling a special number during the registration process.
- **SMS & Surf**

  like self-registration with SMS but the user receives a direct validation link and does not have to enter

username and password. By clicking on the link received, the user completes the validation of his account and can surf the Internet.

- **Click & Surf**

  1-click authentication, which requires the user to make only one click on the access button, taking note of the privacy policy and the terms and conditions.

- **Mail & Surf**

  authentication by email, which requires the user to provide the email address, which is verified with a link sent to the inbox provided by the user.

- **Pay & Surf**

  authentication through the purchase of prepaid packages that guarantee different bandwidth cuts, time etc. Payment is performed directly on the Welcome Page using PayPal.

- **Scratch card**

  authentication based on the insertion of a scratch card number. The scratch cards can be generated from the appropriate panel on the platform and they are delivered to the customer, who, by entering the number, is enabled to navigate.

- **Group code**

  authentication based on a group code, which can be used by multiple users at the same time (particularly useful during meetings and conferences).

- **Social login**

  authentication done using OAuth with an external provider based on the user social account. Supported platforms include: Twitter, Facebook, Google, LinkedIn, Apple and VKontakte;

- **Sponsor login**

  corporate like authentication mechanism: each guest must select a privileged person by specifying his/her e-mail address (in a previously populated list or directory), those people receive an e-mail with all the data of the person who wants to connect and, after having reviewed them, with a simple click they can be authorized;

- **SAML**

  authentication connected to external providers that uses the “Security Assertion Markup Language”;

- **OpenID**

  authentication through third-party accounts interfaced via openID Connect protocol;

- **Roaming**

  authentication through third-party authenticators (e.g. Boingo, iPass etc.);

- **SPID**

  authentication via SPID (the Italian digital public identity system); the Captive Portal is the Service Provider to the different SPID IDP, through a specific license and the accompanying activation activities.

- **eIDAS**

  authentication via the EU regulation electronic identification; like SPID but for all the European citizens.

The methods can be enabled independently of each other and can be turned on and off by the customer.

Note that regarding methods with Social Login, the information collected is only the basic ones for authentication; if the Customer requests to obtain further information, it will be necessary to modify the Social Network APP in this regard, and authorization will still be requested from the Social Network to the end user.

Welcome back manager

The Captive Portal MobiMESH system provides some smart return management methods. The following are all the possible methods, at the customer's choice:

- **Standard Application Authentication**

  the user re-authenticates inside the browser every time he returns to coverage after the expiration of the idle system timeout

- **Welcome back**

  the MAC Address of the device with which it has connected is associated with the user account. When the user returns to the coverage area with the same terminal (therefore with the same MAC Address) within the Welcome Back Timeout window, the system recognizes the MAC Address and assumes that it is always the same user; so the Welcome Page is not shown to re-authenticate, but a Welcome Back Page with simplified access

- **Home-like Wifi**

  It is an evolution of Welcome Back, managed no longer at the application level, but at the network level. At the time of the first login, and for a parametric time defined Home-Like Timeout, the account is associated with the user's MAC Address, in a similar way to what is provided in the Welcome Back mechanism. When the user returns to the coverage area, with the same MAC Address and within the Home-Like Timeout, the system recognizes it and, unlike the Welcome Back, automatically activates the connection.

Navigation policy

- **Static limit**

  the limits that can be set are session timeout, idle timeout, update interval, bandwidth per user in uplink and downlink.

- **Daily limit**

  taxable limits are time, traffic, time and traffic, time or traffic, bandwidth per user in uplinks and downlinks. It is also possible to set the "throttled mode", which provides that when the set constraints are exhausted, you switch to reduced-bandwidth mode until the end of the day;

- **Ticket**

  constraints can be fixed limits (which set maximum bandwidth in downlink and uplink, idle timeout, profile ID, etc.), limits on application NAS, amount of login time, number of logins allowed, expiration date.

Each domain can be associated with a default policy among those described above, with the configured constraints; you can also override the policy per user.

Conclusion

MobiMESH inPiazza platform allows venues to fully exploit their potential and to drive their Customer Journey, through digital and physical touchpoints.

Contact us to learn how MobiMESH inPiazza can deliver a full proximity engagement solution with A.I. business analytics.

More information please visit https://mobimesh.it

Ruckus solutions are part of CommScope's comprehensive portfolio for Enterprise environments (indoor and outdoor).

We encourage you to visit **commscope.com** to learn more about:

- Ruckus Wi-Fi Access Points
- Ruckus ICX switches
- SYSTIMAX and NETCONNECT: Structured cabling solutions (copper and fiber)
- imVision: Automated Infrastructure Management
- Era and OneCell in-building cellular solutions
- Our extensive experience about supporting PoE and IoT

COMMSCOPE®

RUCKUS®

commscope.com

Visit our website or contact your local CommScope representative for more information.