



# PIApoint.campus

04/2004 - V1.0

## Functional Overview

Software Release 3.2.1

The content of this document is copyright protected and intellectual property of:

**DAVOnet GmbH**  
**An der Dorfweise 3**  
**D 35260 Stadtallendorf**

This document and related content can be changed at any time and without prior or further notice.

© Copyright 2004 by DAVOnet GmbH, Stadtallendorf

## Content

<b>1</b>	<b>INTRODUCTION</b>	<b>4</b>
<b>2</b>	<b>STARTING POINT</b>	<b>4</b>
<b>3</b>	<b>FUNCTIONAL OVERVIEW OF PIAPOINT.CAMPUS</b>	<b>4</b>
<b>3.1</b>	<b>TECHNOLOGY</b>	<b>4</b>
3.1.1	SOFTWARE	4
3.1.2	TECHNICAL BASELINE FUNCTIONS	5
<b>3.2</b>	<b>SYSTEM</b>	<b>6</b>
3.2.1	BASELINE	7
3.2.2	WLAN USER PORTAL	7
3.2.3	USER MANAGEMENT	9
3.2.4	ONLINE HELP	9
<b>4</b>	<b>SECURITY</b>	<b>10</b>
<b>5</b>	<b>SYSTEM REQUIREMENTS</b>	<b>10</b>
<b>6</b>	<b>MULTI-CELL WLAN HOTSPOTS</b>	<b>11</b>

## 1 Introduction

This information is intended to provide a quick and brief overview about the functions and features of PIApoint.campus – a comprehensive application for AAA (Authentication, Authorization and Accounting) of corporate, private WLAN (Wireless LAN) networks.

PIApoint.campus is part of the PIApoint family of products and has specifically been designed to meet the needs of corporate WLAN network operators.

The ongoing development of all PIApoint products ensures that your network services are always on the leading edge of today's technology and that your initial investment stays protected for a long time.

Please note that some of the features mentioned here within might be available as options only. Our concept of system-options allows you to choose only what you need and really want.

More detail regarding the features is available upon request.

How to contact us or one of our solution partners can be found on our website <http://www.davonet.de>.

## 2 Starting Point

Operating a corporate or private Wireless LAN network becomes more and more attractive due to the simplicity of installation and the relatively low cost of infrastructure. WLAN networks do help to increase productivity of your employees and do bring us closer to the idea of “every information everywhere and anytime”-

However the advantage of WLAN cannot hide that the operation of a WLAN does have some specific requirements that need assistance – need solutions.

No network administrator really can or wants to manage MAC list on every single Access-Point within the WLAN for every device that should be allowed to get access to the network. More effective, flexible and better ways to control access to the network are needed – ways to better provide user authentication.

Based upon years of experience in the development of software solutions for WLAN hotspots we decided to launch PIApoint.campus to help solving the authentication issues, but also to allow for usage control and accounting.


## 3 Functional Overview of PIApoint.campus

### 3.1 Technology

#### 3.1.1 Software

PIApoint.campus is a really complete software solution. Accordingly you do not only get the application itself but also every software that is needed to install, run and operate the system. All related and used software to build the basis for PIApoint.portal are reliable and stable „Open-Source“ products.

The “Total-Cost of Ownership (TCO)” are thereby really minimized !

PIApoint.portal is based upon **LINUX** . We are using the **Debian** Distribution, widely used on professional webservers.

Other open-source components are

- Apache Webserver
- TOMCAT Servlet Engine
- Java2 Runtime
- Stateful Inspection Firewall

Installation of PIApoint.campus is done very easy and almost automatically. No Linux Know-How is needed at all. The excellent documentation leads you through all steps and informs about everything needed to know.

The entire configuration and administration is web-based. This means that you manage your system very comfortable using your web-browser. This also allows to easily manage your hotspot remotely and to save cost for monitor and keyboard on your hotspot server running on PIApoint.portal.

If you do not want to do the installation on your own – you also can decide for a pre-installed appliance server system – almost plug-and-play with only minor settings to be made by yourself locally.

3 different appliance servers are available – depending on your performance needs – on the number of parallel users especially.

### 3.1.2 Technical Baseline Functions

The most important, technical functions of PIApoint.portal are:

- Intranet Server and User-Portal within your local area network / Hotspot (Captive Portal)
  - Own, configurable, internal Domain-Name Server for your WLAN ([www.company.wlan](http://www.company.wlan))
- DHCP Server integrated
  - Configurable IP Address areas (Start- / End-DHCP / Lease-Time etc.)
- DNS Proxy integrated
  - Allowing to integrate other internal servers e.g. the Intranet-Server of your company
- NAT Router integrated
  - Even WLAN clients with static IP address-settings are supported
- MAC Address authentication
  - Allows „n“ MAC addresses to use the hotspot without UAM (Username/Password) authentication. These devices are automatically authenticated – all across your entire WLAN with only 1 central pool of MAC information to be maintained-
- Internet Router integrated
  - PPPoE DSL Router (simply connect to your ADSL Modem)
  - ISDN Router (requires AVM-ISDN Card)
  - LAN / WAN Router (supports even Highspeed SAT-connections, e.g. Eutelsat)
  - Integrated Stateful Inspection Firewall
- Proxy Integration
  - Allows to integrate existing Proxy Servers without need to change proxy-settings
    - Content Filtering
    - Web Cache
- VPN Router - Multi-Session and Multi-Protocol (IPsec, PPTP, OpenVPN a.o.)
  - Secure VPN connections for hotspot users
    - No need for fixed IP addresses on the internet (intelligent NAT)
    - Add the VPN host to your “walled Garden” and allow all users to use highly secure VPN connections to your internal servers without any prior user-authentication – if not added to walled-Garden the user first needs to authenticate himself on PIApoint.campus before he can establish a secure VPN connection.

- 2 Bandwidth Management Options
  - Stochastic bandwidth leverage and distribution across all users online (Fair-Share) and
  - Configurable Up- and Downstream bandwidth for your entire WLAN or on a per user setting (Bandwidth-Limiter)
- Session Controller
  - Automatic Session-Timeout and Logout of inactive user sessions
  - AccessPoint Cell Roaming – User sessions stay connected even when changing cell-sites in your WLAN (Cell Roaming)
- AAA Server
  - Using IP Layer 3 functions – therefore to be used with all IP compliant networks (Ethernet, PowerLAN, VDSL and WLAN)
  - Authentication by
    - UAM ( User-ID / PIN to be entered online)
    - RADIUS Server integration
    - IEEE 802.1x (MD5, PAP, MS-CHAP V2) if also supported by Access Points
      - EAP-TLS and EAP-TTLS under construction available soon
  - Authorization by predefined firewall rule tables
    - Limitation of ports and protocols to be used within the WLAN
  - Accounting
    - Collection of usage records per User, per Account
    - Define Time and Volume limits on a per user basis
- RADIUS Gateway to handle external AAA requests
  - Realm-Authentication and accounting (username@provider.xx, Password)
- Accounting Server
  - time based usage accounting
    - Account expiration x-hours after first login, or
    - Account expiration after x-hours effectively used time online
    - Online info about available account-balance
  - Volume based accounting
- XML interface to specifically integrate Nomadix devices, if needed at all

## 3.2 System

The system administration provides you comfortable and easy-to-use web-based access to all important system parameters. You can manage your hotspot from any PC within the LAN or even from outside – using the remote access functionality.



### 3.2.1 Baseline

Easy configuration of the Internet access ( LAN, DSL, ISDN)

- Systemdate and –time
- Restart Webservices / Shutdown system
  - Online-Check of Logfiles
- Backup and Restore of system settings
- Define your personal, internal WLAN domain-name
- Homepage-Link for free access to your homepage in the internet
- Walled Garden Definition – free access to configurable internet domains
- WLAN – Intranet configuration
  - IP address
  - DHCP Start- and End
  - WLAN Broadcast IP Address
  - DHCP IP lease time
  - WLAN Domain-Name
  - Portal Protocoll (http / https)

#### Note:

We recommend to use SSL for encryption of logon-data transferred between user client and the portal page. This complies with the hotspot security recommendations of „Verbands der deutschen Internetwirtschaft, eco e.V.“ The system contains a private 128bit SSL certificate. Official certificates can be used either.


- RADIUS Gateway configuration
  - Connection and SSL Encryption to PIApoint.integrate Server and Backup-Server
- Remote Access configuration
  - Definition of a Dyn-DNS Server, Name, User etc.
  - SSH Port definition
  - Generation of SSL certificates

### 3.2.2 WLAN User Portal

This picture shows a sample of how the standard portal page looks like. The WLAN user will, if not already authenticated and authorized e.g. using MAC list or 802.1x authentication, automatically be routed to this page. The picture shows where you easily can adjust the page to your personal needs. Simply load your own pictures up to the system – no programming, no html is needed.

If desired you can also define any existing individual page to “welcome” the user. If this page is hosted on the Internet, the respective www address is automatically added to the Walled-garden of PIApoint.campus.



- Enter your individual logo / graphics onto the portal page
  - Or select any existing website within the Intranet or Internet to be used
  - further options to adjust the page are given using style-sheets.
  -  PIApoint.portal hotspots can be used with almost all PDA
    - Special page for most PDA browsers included
- Upload new licence information and software updates
  - Software Licence Upgrades z.B.
    - More parallel users
    - More features, functions and options
- Upload own text information for the user
  - Terms & Trades of use
  - General Info
- Configure default language of the portal page and administration
  - Available : German, English, Spanish and Italian
- Online Info about
  - Version of software
  - Available options etc.
- FAQ Link to DAVOnet Website
- Extensive Online Help (PDF)

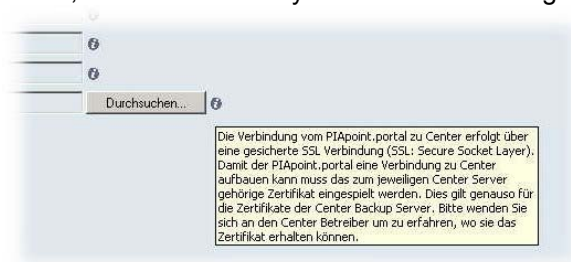
### 3.2.3 User management

These functions are used for day-to-day operation:

- Create new, local user accounts ( User-IDs and PINs )
- Configure „Free Access“ - time-barred access with dynamically created userid/PIN
  - 10 or 30 minutes per day and MAC address
- Configure Group-accounts
  - Online generation of a User-ID and Password valid for 24h after first use. N-Users can then in parallel use the code information to log on. Ideal for congresses and events with multiple parallel users.
  - Online deactivation of group account
  - Shell-Script based, automatic configuration and deactivation
- Configuration of MAC Authentication
  - Define MAC Addresses that can use the hotspot without need to log on and to use existing prepaid accounts etc.
- Online Account Information
  - How many accounts are existing
  - What is the time-balance per account
  - IP Adresse, MAC Adresse, balance of accounts currently used
- Passwort-Reset of user account

### 3.2.4 Online Help

The Online Help information covers the entire system manual. Additionally there are add-on information easy to get by clicking in „i“ symbols on the web-interface. You really do not need to be an IT expert to install, run and use the system to better manage your hotspot business.



## 4 Security

Security is a very important issues for us and for your WLAN and users as well. PIApoint products comply with commonly accepted security standards and are therefore accepted by professionals all around the world.

- Integrated Stateful Inspection Firewall
- SSL encrypted user login
- SSL encrypted communication with external roaming gateways – RADIUS servers
- SSH encrypted Remote-Shell administration
  - Supports to use Dyn-DNS services
- Automatic Session Time-Out if user is inactive for longer than 5-15 minutes
- VPN Support (IPsec, PPTP, OpenVPN)
- UAM Authentication requires User-ID and PIN/Password to logon
- 802.1x Authentication optionally by adding PIApoint.integrate to handle communication between Access-Point, RADIUS-Server and PIApoint.campus
- Optional RADIUS Authentication using existing User-Ids and PINs residing on an existing RADIUS Server
  - The logon Window will automatically be expanded
  - The Realm select box will automatically be filled with valid @-Realm information



## 5 System requirements

If yo do not decide for our Plug-and-Play solution where you get a already installed and widely ready-to-use WLAN package , you need to have at minimum the following platform ready for installation of PIApoint.campus

### Server - Hardware:

- PC, Processor AMD Duron or Intel Celeron 300 MHz or better
- RAM min. 64 MB or better ( +64 MB per +10 users recommended)
- HDD (IDE): min. 20 GB
- Keyboard (only for software installation needed)
- 2 network connector cards <sup>1)</sup>
- CD-ROM (IDE) <sup>2) 3)</sup> (only during installation)
- VGA and Monitor (for installation only)

## 6 Multi-Cell WLAN Hotspots

PIApoint.campus supports Cell-Roaming!

This means that your user can really walk around within your WLAN covered area, without losing his sessions and connections. He can roam from one radio-cell-site to another. Your WLAN can grow as much as you need and want – there are no additional cost per Access-Point etc!

And remember – your network is not limited on WLAN only – you can use PIApoint.campus with any IP technology and even combine those, just as it is needed.

