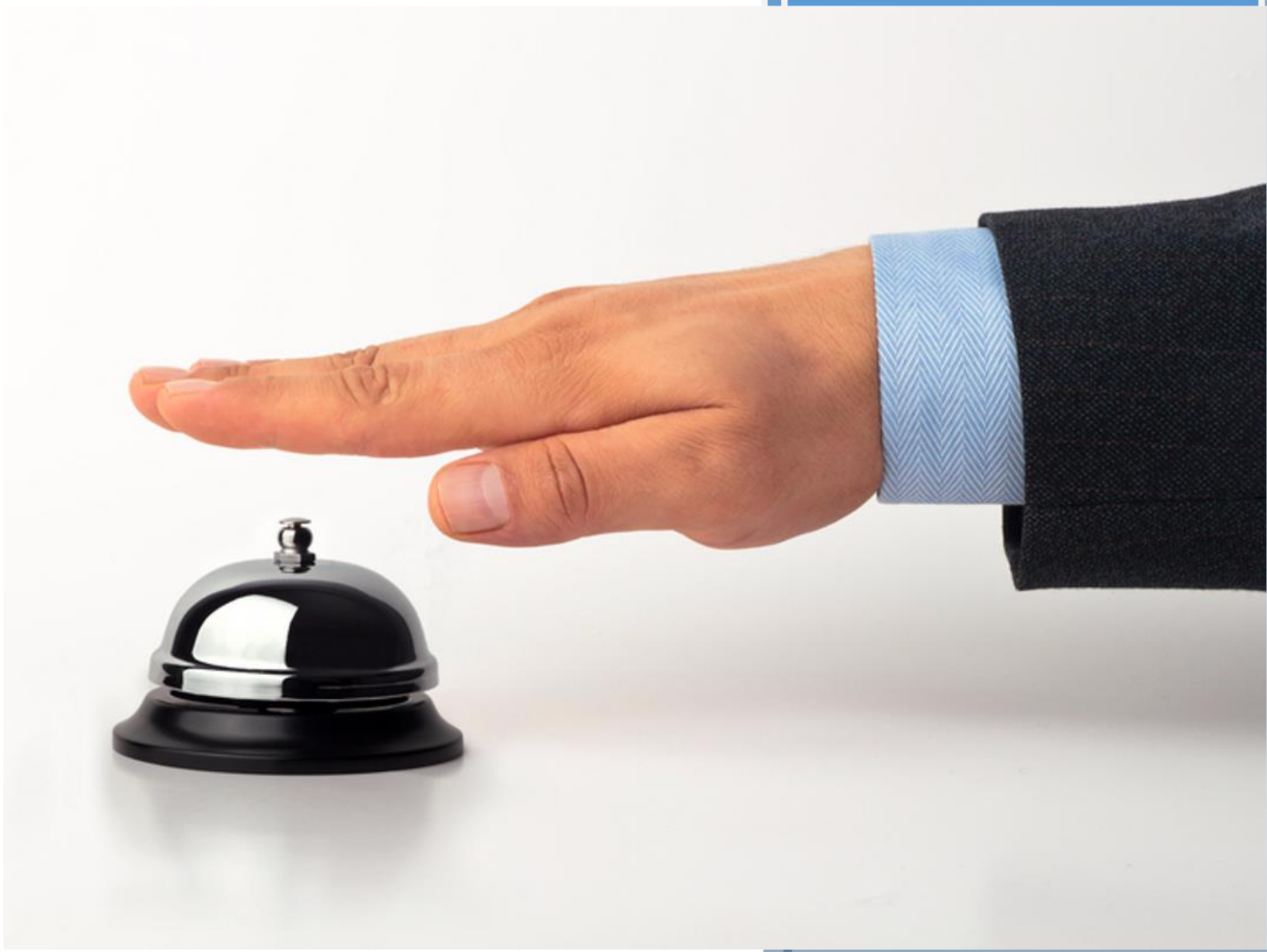
PSE

User manual – HSC Hot Spot



1 Internet for Guests

1.1 Your Registration Number:

1.2 Disclaimer

The information provided in this brochure contains merely general descriptions or characteristics of performance which in case of actual use do not always apply as described or which may change as a result of further development of the product. An obligation to provide the respective characteristics shall only exist if expressly agreed in the terms of contract. Availability and technical specifications are subject to change without notice.

Windows® is a registered trademark of Microsoft Corporation in the United States and other countries.

Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

Java® is registered trademarks of Oracle and/or its affiliates

All other company, brand, product and service names are trademarks or registered trademarks of their respective holders.

PSE makes no warranty, express or implied, in fact or in law, including, but not limited to any implied warranties of merchantability or fitness for a particular purpose. Warranty information and services for non-PSE products can be found on the manufacturer's website or is provided with the equipment. In no event shall PSE and/or its respective suppliers be liable for any special, indirect or consequential damages arising from the use of PSE products.

1.3 Notes

2 General Information

2.1 About the Product

Thank you for choosing 'Internet for Guests'. The system enables you to provide guests with an Internet connection using 'Surftickets' within the 'Surf-LAN' (dedicated network for your guests). To administer the system with the so-called 'WebAdmin', you'll only need a web browser (e.g. Internet Explorer, Firefox, Safari, etc.) installed on one of the computers in the 'Office-LAN' (your office network).

In addition, the system has a range of other benefits:

- real Plug and Play (no amendments to or software installation on the end-device)
- simple creation of freely definable 'Surftickets'
- billing based on volume and/or time
- multi-language capability
- integrated security features (Firewall, Web Filter, etc.)
- many useful modules (e.g. Online Update, 'PMS' Connector)
- and much more ...

Have a good time.

2.2 Implementation

	The 'Office-LAN' is protected by an integrated firewall. This ensures that your office network is completely separate from your guests.
	Using a convenient bandwidth management, you can allocate only a part of your Internet bandwidth to your guests and still guarantee a trouble-free Internet connection for your office operations.
	You will need to comply with any national legal regulations and to configure the system appropriately.
	The system is best placed in a server, or system, room. Protect the device from dust and the effects of heat.

2.2.1 Requirements

To be able to use 'Internet for Guests' you'll need to have:

- broadband Internet access (e.g. DSL, Cable)
- network infrastructure (e.g. CAT5, WLAN, Powerline)
- DSL/cable router
- web browser to administer 'Surftickets'

If the system is installed behind a firewall, as well as the standard port such as HTTP, DNS, etc. you will need to permit additional connections to the following ports:

Value	**Description**
53 TCP/UDP	Domain Name Service (DNS)
123 TCP/UDP	Time Server (NTP)
873 TCP/UDP	Online Update
1194 TCP/UDP	Central Services VPN
5555 TCP	Remote Control

2.2.2 System Default

The system has the following network settings for 'Office-LAN' by default:

Value	**System Default**	**Note**
IP Address	192.168.1.1	IP address of the system within the 'Office-LAN'
Subnet Mask	255.255.255.0	subnet mask of the 'Office-LAN'
Default Gateway	192.168.1.254	default gateway (usually DSL router, cable router, etc.)
Time Server (NTP)	ntp.frozentux.org	NTP / Time Server for time synchronization (e.g. ntp.frozentux.org)
Primary DNS Server	192.168.2.1	server for DNS requests (e.g. settings like other devices within the 'Office-LAN' / provider DNS)
Secondary DNS Server		server for DNS requests (e.g. settings like other devices within the 'Office-LAN' / provider DNS)

The 'Surf-LAN' DHCP range is configurable from 172.30.0.0/17 to 172.30.0.0/22. In the 'Surf-LAN', the system can be addressed by using 172.30.3.254.

The 'Surf-LAN' has to occupy a different IP/subnet area than the 'Office-LAN'.

2.2.3 Integration

The hardware contains two network cards and can be connected to the company network -

after being installed and configured - as follows:

Integration

1. Network Card: 'Office-LAN'

Using the patch cable, connect the network card labeled 'Office-LAN' on the system with your office network (e.g. Switch, DSL router). The configured system now uses the existing office network's Internet connection.

Wherever possible, the 'Office-LAN' should not be a classic network (e.g. 192.168.0.x, 10.0.0.0, 172.16.0.0), because computers in the 'Surf-LAN' that are in the IP area of the 'Office-LAN' will not find a Plug and Play environment (change network settings of device to DHCP). This can happen if guests have set the same classic network in their home or office network.

2. Network Card: 'Surf-LAN'

Using the patch cable, connect the network card labeled 'Surf-LAN' on the system with the guest's network (e.g. Switch, WAP).

The 'Surf-LAN' can be structured in a number of ways. Possible variations include:

- as direct start, a single wireless access point
- CAT5 Ethernet cabling
- HomePNA
- VDSL

- etc. or in combination

	Make sure that the 'Office-LAN' and 'Surf-LAN' network connections are not mixed up - this can severely damage the office network.
	In contrast to a wireless access point, a WLAN router allows all device behind the router to become active with just a single 'Surfticket'. This can be by-passed by switching to a so-called 'bridging mode'.

3 Administration with 'WebAdmin'

	The connection to the web interface is encrypted for security reasons.

After installation the system can be fully administered using a web interface.

In the installation process the IP address of the office network to the system has been allocated. Now use the web browser in your office network to open the web interface. To do this type in the https (= secure protocol) and the IP address of the system (e.g. https://192.168.1.1). To access the program quicker in future bookmark the link.

Please contact your system administrator for further information.

Confirm the security prompt (e.g. Yes, Continue to this website). The 'Internet for Guests - WebAdmin' logon appears.

The system has two predefined users.

	System Administrator [Username: sysop] [Default Password: sysop]
	Ticket User [Username: ticket] [Default Password: ticket]
	Please note that Username and Password are case sensitive.
	For security reasons, please change password.

3.1 Tickets

3.1.1 Create

You get an user/password combination on the generated 'Surfticket', with which your guests have access to the Internet for a selected time period and/or Internet traffic. Select your required template first to display all ticket values. By clicking on Save, the print dialog opens.

For security reasons, a user must have administrator rights to modify all values.

Value	**Description**
Template Name	Name of selected template.
Ticket Type	• FLAT RATE: In a defined time window (e.g. 6 days after first logon) a defined amount of data can be used. This is independently of the time it is consumed. • TIME RATE: The surf duration printed on the 'Surfticket' can be used minute-exactly by logging on and off.
Time Credit	Defines the time in minutes, hours, or days, a ticket is valid (e.g. 30 minutes).
Session Limit	Defines the download volume in megabyte a user can consume per session (e.g. 50 MB).
Ticket Limit	Defines the download volume in megabyte a user can consume for the entire ticket (e.g. 100 MB).
Valid from/to	Defines the period of time a user can consume the time credit (e.g. from 01.01.2000 to 31.12.2099).
Max Download Bandwidth	Defines the maximum download bandwidth for the 'Surfticket'.
Max Upload Bandwidth	Defines the maximum upload bandwidth for the 'Surfticket'.
Ticket Price	Defines the price of the 'Surfticket'.
Ticket Language	Select the ticket language (e.g. German, English).
Max Devices	Maximum number of devices which can be logged in simultaneously.
Fixed Bandwidth	Information whether the selected ticket template has set a fixed bandwidth or not.
Allowed VLANs	Displays all VLANs which are valid for the selected ticket template.
Print to	Select if you want to print to office printer or ticket printer (if defined) or send the ticket data via SMS or Email.
Description	Description for the 'Surfticket' (e.g. Mr. Schneider, Room Nr. 104).

3.1.2 Users

Create reusable tickets with static username and password including multiple logins with same username.

Use this feature for example for conventions.

Value	**Description**

Username	Enter a username.
Password	Enter a password which can be fixed or random generated.
Description	Enter a description.
Name	Users real name (optional).
Email	Users email address (optional).
Ticket Template	Assigned ticket template to successfully authenticated users.
Max Users	Maximum number of users that can login simultaneously with same username and password.
Shared Limits	• checked: Ticket limits provided by template are shared among multiple users. • unchecked: Every login user obtains the ticket limits provided by template.
Fixed Bandwidth	Check to activate fixed bandwidth for the selected user.
Renew	Ticket will automatically renew after expiration (e.g. ticket limit exceeded). • now: immediately • daily: daily at 00:00 • weekly: weekly on Monday at 00:00 • monthly: monthly on first day of month at 00:00 • yearly: yearly on 01.01. at 00:00 • never: never - to renew manually interaction required
Valid from	Login only valid from date.
Valid to	Login only valid to date.
Active	Activate user.
Create	Create new ticket for user.

Copy

Copy settings of existing user.

Settings

When activated, the password policy settings can be set for each user individually or global for all users.

Value	**Description**
Change password at next logon	If activated, all users are forced to change their passwords at next logon.

Value	**Description**
Change password every	Number of days after a password change will be forced to the users.
Min. password length	Defines the minimum password length.
Password Policy active	Choose the password policy setting for this user. • Default: Uses the global password policy settings. • Deactivated: No password policy for this user. • Custom: Define custom password policy settings for this user.

3.1.3 Manage

You can view the 'Surftickets' that have already been generated. Depending on the choice made (used, unused, online, expired, all, search criteria), you'll see a list of the available tickets.

	The details view could help to clear up guest queries (guest complains, for example that he/she can no longer surf the web). A possible solution might be that the ticket limit has been used up.
	For security reasons, a user without administrator rights can only cancel unused tickets / can not display Connection Tracking.

Action	**Description**
Details	All ticket-related information can be called up with the help on the details view. Here, you can also see when the guest logged on or off.
HTTP Proxy	(if activated) Displays the proxy server log entries of selected 'Surfticket'.
Connections	(if activated) Displays the connection log entries of selected 'Surfticket'.
Print	Print out a copy of selected 'Surfticket'.
Revoke	If a ticket has been mistakenly issued or misused, it can be deactivated by pressing the Revoke button. It is no longer possible for the guest to logon with this 'Surfticket'.
Renew	Renews a revoked or invalid ticket by creating a valid copy of the ticket.

3.1.4 Bulk

The creation of bulk tickets makes it possible to create a large number of 'Surftickets'. After pressing Save, the file (a common CSV file format) with the access data in the area below can be downloaded for further processing. If one deletes a file, the generated 'Surftickets' are not affected.

	The bulk creation is ideal if you want to distribute 'Surftickets' with username/password to your guests with serial letters, on scratch cards, in bulk eMails, etc.
	For security reasons, a user must have administrator rights to modify all values.

Value	**Description**
Template Name	Name of defined template.
Ticket Type	• FLAT RATE: In a defined time window (e.g. 6 days after first logon) a defined amount of data can be used. This is independently of the time it is consumed. • TIME RATE: The surf duration printed on the 'Surfticket' can be used minute-exactly by logging on and off.
Time Credit	Defines the time in minutes, hours, or days, a ticket is valid (e.g. 30 minutes).
Session Limit	Defines the download volume in megabyte a user can consume per session (e.g. 50 MB).
Ticket Limit	Defines the download volume in megabyte a user can consume for the entire ticket (e.g. 100 MB).
Valid from/to	Defines the period of time a user can consume the time credit (e.g. from 01.01.2000 to 31.12.2099).
Max Download Bandwidth	Defines the maximum download bandwidth for the 'Surfticket'.
Max Upload Bandwidth	Defines the maximum upload bandwidth for the 'Surfticket'.
Ticket Language	Select the ticket language (e.g. German, English).
Ticket Price	Defines the price of the 'Surfticket'.
Max Devices	Maximum number of devices which can be logged in simultaneously.
Quantity	Number of tickets to create.
Description	Description for the 'Surfticket' (e.g. Mr. Schneider, Room Nr. 104).
File Upload	Allows you to upload a text file with predefined usernames and passwords.
File	Only visible if ”File Upload” is checked. Select the file to upload.
Delimiter	Only visible if ”File Upload” is checked. Select the delimiter which is used in the file to separate usernames and passwords.

File format example for file upload.

Line #	**Example entry**
1	Username1;Password1;Description1

Line #	**Example entry**
2	Username2;Password2;Description2
3	Username3;Password3;Description3
4	Robert;12345;Ticket Robert
n	USERNAME;PASSWORD;DESCRIPTION

Download

Value	**Description**
Details	Shows bulk ticket details (e.g. language, quantity).
Download	Download list of bulk tickets as CSV file.
View	Show overview and print bulk tickets.
Revoke	Revokes all bulk tickets.

3.1.5 Templates

Any number of templates can be defined which you can select when creating an 'Surfticket'.

Enter 0 for Ticket Limit or Session Limit to get system default (Settings/Ticket).

Templates - Overview

Create, edit and delete ticket templates.

Value	**Description**
Template Name	Name of defined template.
Description	Description of service (e.g. 30 minutes per day). Description will be displayed on landing page.
Prefix	If ”System Default” is checked, the default ticket prefix from menu ”Settings/Ticket” will be used. Otherwise the user can define his own ticket prefix in the field behind.
Ticket Type	• FLAT RATE: In a defined time window (e.g. 6 days after first logon) a defined amount of data can be used. This is independently of the time it is consumed. • TIME RATE: The surf duration printed on the 'Surfticket' can be used minute-exactly by logging on and off.
Time Credit	Defines the time in minutes, hours, or days, a ticket is valid (e.g. 30 minutes).
Session Limit	Defines the download volume in megabyte a user can consume per session (e.g. 50 MB).
Ticket Limit	Defines the download volume in megabyte a user can consume for the entire ticket (e.g. 100 MB).

Value	**Description**
Expiration Period	Defines the days a user can consume the time credit (e.g. 365 days).
Ticket Price	Defines the price of the 'Surfticket'.
Max Download Bandwidth	Defines the maximum download bandwidth for the 'Surfticket'.
Max Upload Bandwidth	Defines the maximum upload bandwidth for the 'Surfticket'.
Fixed Bandwidth	Check to activate fixed bandwidth for the selected ticket template.
Max Idle Time	Time span in minutes after an inactive session (e.g. no network traffic) is automatically logged off.
Max Devices	Maximum number of devices which can be logged in simultaneously.
Allowed VLANs	Select specific VLANs for which the selected ticket template is valid.
Data Collector Template	Select a data collector template to collect additional information like Email address, name etc. about the user. Data collector templates can be defined in menu ”Settings/Ticket”.
User Group	If one or more user group is activated, you can select whether all user groups, only one specific user group or none of them can create tickets based on this ticket template.
Bypass Web Filter	If web filter is activated, check to bypass web filter for this ticket template. Tickets based on this ticket template are not web filter restricted.
WebAdmin	(if available) Activate the box to make the selected template available for the module.
Ticket Printer	(if available) Activate the box to make the selected template available for the module.
Authentication	(if available) Activate the box to make the selected template available for the module.
Multimedia	(if available) Activate the box to make the selected template available for the module.
Email	(if available) Activate the box to make the selected template available for the module.
PMS	(if available) Activate the box to make the selected template available for the module.
Article#	Can only be used for PMS types which support article number posting. If not supported, this field will be ignored.
Online Payment	(if available) Activate the box to make the selected template available for the module.
Public IP	(if available) Activate the box to make the selected template available for the module.
SMS	(if available) Activate the box to make the selected template available for the module.

Value	**Description**
Social Login	(if available) Activate the box to make the selected template available for the module.
Logon Hours	Select certain hours/days where this ticket template can not be used/can be used only.

Templates - Sort Order PMS / WebAdmin / Online Payment

Allows you to sort the display order of the available tickets on the client logon page by drag and drop.

Free Logon

Free Logon allows you to offer free internet access per MAC address (e.g. 30 minutes for free per day).

Value	**Description**
Time Credit	Defines the time in minutes, hours, or days, a ticket is valid (e.g. 30 minutes).
Ticket Limit	Defines the download volume in megabyte a user can consume for the entire ticket (e.g. 100 MB).
Max Idle Time	Time span in minutes after an inactive session (e.g. no network traffic) is automatically logged off.
Repeat Interval	Timespan after expiration when service is available again for customer (e.g. 60 minutes).
PMS Authentication required	PMS Authentication required to use service (if PMS system is present).
VLAN Based	If checked, the free logon template can be activated for individual VLAN's.
Description	Description of service (e.g. 30 minutes per day). Description will be displayed on landing page.
Max Download Bandwidth	Defines the maximum download bandwidth for the 'Surfticket'.
Max Upload Bandwidth	Defines the maximum upload bandwidth for the 'Surfticket'.
Max Repeat	Defines the maximum number a device can use this service (e.g. 1 = device can use this service only once).
Data Collector Template	Select a data collector template to collect additional information like Email address, name etc. about the user. Data collector templates can be defined in menu ”Settings/Ticket”.
Show as Sign Up	Show the free logon button as sign up button together with the social login buttons.
Expires after Logout	If checked, the free logon ticket expires automatically after the user logs out manually or gets logged out by the idle timeout.

PMS: Groups

Create VIP groups and assign specific VIP ticket templates. (This feature must be supported by your configured PMS)

Value	**Description**
Create	Create a new VIP group.
Name	Enter a name for the VIP group.
Description	Enter a description for the VIP group.
Templates	Assign ticket templates to the VIP group which then can be used by this VIP group only.
Edit	Edit the selected VIP group.

The system default group can not be deleted. All ticket templates which should be visible for ”normal” user (non VIP user) must be assigned to this group.

PMS: VIP Guest - Free Logon

Defines a VIP Template which is used for Guests with VIP status. (This feature must be supported by your configured PMS)

Value	**Description**
Name	Name of the VIP template.
Ticket Limit	Defines the download volume in megabyte a user can consume for the entire ticket (e.g. 100 MB).
Max Idle Time	Time span in minutes after an inactive session (e.g. no network traffic) is automatically logged off.
Description	Enter a description for the VIP template.
Max Download Bandwidth	Defines the maximum download bandwidth for the VIP template.
Max Upload Bandwidth	Defines the maximum upload bandwidth for the VIP template.

3.2 Client Logon

3.2.1 Terms of Use & Help

Text box for each language to enter your terms of use which will appear at the logon page. If a language has been deleted, the default language will be shown. All languages can be reset to delivery status.

Customize help text for the customer logon page according to your needs.

A default help text is available in english and german. For further languages, the translations must be done by yourself.

3.2.2 Free to Use

Define free accessible websites without logon (either visible or hidden on logon page).

	Give your guests free access to your own website, the platform of the local tourist board, etc.
	For HTTPS sites no wildcards or subdirectories are allowed. Only use hosts (e.g. https://www.ssl-secured.com).

Upload URL List

Allows you to upload a text file with Free to Use URLs.

	Define one URL per line. Valid field delimitors are: ';' and ','

File format description:

Field #	**Field name**	**Value type (range)**	**Field description**
1	URL	string	URL for free to use URL.
2	Description	string	A short description about the URL (not required for hidden free to use links).

File format example:

Line #	**Example entry**
1	http://www.example.com;My Example Website
2	http://www.example2.com,My 2nd Example Website
3	http://www.hidden-example.com
4	https://www.ssl-secured.com
5	tcp://10.2.3.4
6	udp://10.2.3.5
7	tcp://10.2.3.6:80
8	udp://10.2.3.6:8012
n	URLn;DESCRn

Page Dependency Analyzer

The Page Dependency Analyzer displays all referring scripts, images and links of the defined website including hyperlinks to other pages. All scripts, images and links are required to display the defined Free to Use website correctly. Adding the hyperlinks is not required.

3.2.3 Redirect

Redirect after logon

Redirect guests after logon either to his/her default website or to a specified website.

Redirect before logon

Redirect guests before logon to a specified website.

	You need to define ”Free to Use” or ”Hidden Free to use” access to the configured sites (via menu: Client Logon).
	If VLAN is activated, you are able to define different redirect sites for different VLAN ID’s. So you can redirect wired or WLAN guests to different websites. Simply select the url number in VLAN definition.

3.2.4 Logo

The logo will appear on top of the customer logon page.

3.2.5 Design

General - Logon order

The logon order defines the order of the different logon options and also allows you to disable logon options.

General - Display

Value	**Description**
Headline	Edit headline of customer logon page.
Welcome Message	Display welcome message and edit welcome text.
Status Information	Display status information.
Free to Use	Display free to use.
Footer	Display footer.
Advanced Error Message	Activate to enter an advanced error message (e.g. Please contact the reception desk).
Status Information Popup	Activate to show a status popup after login at the customer logon page.

Themes - List

Here you can activate the different themes, edit them (both mobile and standard), export and delete them.

Value	**Description**

Value	**Description**
Standard	Edit the default customer logon page.
Mobile	Edit the customer logon page for mobile devices (e.g. mobile phones).
Delete	Delete the selected theme.
Activate	Activate the selected theme.
Export	Export the selected theme to import it at another HSC HotSpot.

Themes - New Theme

Create new themes for customized customer logon page. Therefore enter a name and select a template.

Themes - Import Theme

Select a theme and import it. Then activate it at the themes list to use it on this system.

Themes - Design

Change the logon design style and switch from system default to custom design. The custom design can be modified by editing HTML templates and CSS files via FTP access.

FTP server start in menu System / Services is required.

Mobile - Display

Show or hide the company logo for the mobile logon site.

CSS Editor

Click on the element you want to change. A CSS editor opens where you can edit all CSS attributes for the selected elements and other similar elements.

CSS knowledge is assumed to edit the themes.

Value	**Description**
Preview	Shows a preview of the customer logon page with the current settings.
Mobile	Edit mobile theme.
Back	Close the theme editor.

3.3 Settings

3.3.1 General

Change the settings of the system to meet your requirements.

The settings should be made by your IT partner as part of the installation process. To make changes, please follow the instructions of your system administrator.

Value	**Description**
Company Name	Name of your company/organisation.
Company Address	Address of your company/organisation.
Company Website	Website of your company/organisation.

System

Value	**Description**	**System Default**
Operation Mode	• 'Normal': pay mode; ticket-based Internet access; guests have to buy a 'Surfticket'. • 'Freelogon': free Internet access for all guests; logon page appears with the button: Access the Internet for free. • 'Autologon': the same as 'Freelogon', but guests log on directly in the Internet.	Normal
Currency	Abbreviation of the currency (e.g. EUR, USD).	EUR
Time Zone	Select your time zone.	
Keyboard	Keyboard layout for the system console.	
Seamless Roaming	If activated allows a valid online user to roam seamless between interfaces on the same end device (e.g. switching from wired to wireless).	activated
Remember me	If a user gets logged off due to inactivity, he will get logged on again automatically as soon as he is active again. This feature is not working if user logs off manually (e.g. logoff button).	activated
Remember Username	Automatically saves the last logged in username at ticket logon. This way the user only has to enter his password at the next ticket logon.	deactivated

3.3.2 Network

Change the settings of the system to meet your requirements.

The settings should be made by your IT partner as part of the installation process. To make changes, please follow the instructions of your system administrator.

Network - General

Edit general network settings.

Value	**Description**
Hostname	Enter a new hostname for customer logon page.
Domainname	Enter a new domainname for customer logon page.
Primary DNS Server	Server for DNS requests (e.g. settings like other devices within the 'Office-LAN' / provider DNS).
Secondary DNS Server	Server for DNS requests (e.g. settings like other devices within the 'Office-LAN' / provider DNS).
Time Server (NTP)	NTP / Time Server for time synchronization (e.g. ntp.frozentux.org).

Network - Office-LAN (eth1)

Edit network settings for 'Office-LAN'.

Value	**Description**
IP Address	IP Address of the 'Office-LAN' interface.
Subnet Mask	Subnet Mask of the 'Office-LAN'.
Default Gateway	Default Gateway (usually DSL router, cable router, etc.).
MTU Size	Edit MTU size for 'Office-LAN'.
Routes	Click to get to the routing configuration.
WebAdmin Access	Activate to get 'WebAdmin' access from 'Office-LAN'.
FTP Access	Activate to get FTP access from 'Office-LAN'.
SSH Access	Activate to get SSH access from 'Office-LAN'.

Network - Surf-LAN (eth0)

Edit network settings for 'Surf-LAN'.

Value	**Description**
IP Address (Unprotected Mode)	IP Address of the unprotected 'Surf-LAN'.
Subnet Mask (Unprotected Mode)	Subnet Mask of the unprotected 'Surf-LAN'.
IP Address (Protected Mode)	IP Address of the protected 'Surf-LAN'.
Subnet Mask (Protected Mode)	Subnet Mask of the protected 'Surf-LAN'.
DHCP Server	Click to get to the DHCP configuration.
Routes	Click to get to the routing configuration.
MTU Size	Edit MTU size for 'Surf-LAN'.
WebAdmin Access	Activate to get 'WebAdmin' access from 'Office-LAN'.
SSH Access	Activate to get SSH access from 'Office-LAN'.

Network - Management-LAN (eth2)

Edit network settings for 'Management-LAN'.

Value	**Description**
IP Address	IP Address of the 'Management-LAN' interface.
Subnet Mask	Subnet Mask of the 'Management-LAN'.
Routes	Click to get to the routing configuration.
MTU Size	Edit MTU size for 'Management-LAN'.
WebAdmin Access	Activate to get 'WebAdmin' access from 'Office-LAN'.
FTP Access	Activate to get FTP access from 'Office-LAN'.
SSH Access	Activate to get SSH access from 'Office-LAN'.

Network - Surf-LAN Certificate

If default Hostname or Domainname is changed you need to upload your own SSL certificate. Therefore you can generate your own CSR and key file using the CSR generator.

Value	**Description**
Status	Shows the validation status of the SSL certificate (green = valid).
Certificate File	Select certificate file for upload.
Certificate Key File	Select certificate key file for upload.
Certificate Authority File	Select certificate authority file for upload (if required by SSL certificate).

Bandwidth Management

Edit total bandwidth settings for 'Surf-LAN' or completely deactivate the bandwidth management.

Value	**Description**	**System Default**
Status	Shows the service status.	Service running
Total Download Bandwidth	Maximum bandwidth in Kbit/s available to all simultaneous surfers (guests).	2048
Total Upload Bandwidth	Maximum bandwidth in Kbit/s available to all simultaneous surfers (guests).	2048
Fixed Bandwidth	Activate to use a specific part of total bandwidth as fixed bandwidth.	Deactivated
Fixed Download Bandwidth	Reserve a part of the total bandwidth as fixed download bandwidth.	Deactivated
Shared Download Bandwidth	Shows the remaining download bandwidth which will be shared among normal users.	Deactivated
Fixed Upload Bandwidth	Reserve a part of the total bandwidth as fixed upload bandwidth.	Deactivated

Value	**Description**	**System Default**
Shared Upload Bandwidth	Shows the remaining upload bandwidth which will be shared among normal users.	Deactivated

SMTP Server

Define an SMTP server to forward emails.

Value	**Description**
Status	Shows the service status.
Sender	Enter the email address of the sender.
Server	Enter SMTP server of your provider.
Port	Enter port of the SMTP server (default:25).
TLS	Enable data encryption using transport layer security (if supported by remote SMTP server).
SSL	Enable data encryption using secure socket layer (if supported by remote SMTP server).
SMTP Authentication	If SMTP authentication is required, enter username/password to authenticate on remote SMTP server.
Testmail	Send a testmail to check if SMTP configuration works.

SMTP Proxy

Most ISPs (Internet Service Providers) not allow sending eMails from a non-customer account. Most of your customers can receive (POP-Server) their eMails but not send them (SMTP-Server) because they are connected with your ISP. Enter your SMTP Relayhost to enable customers to send eMails via your ISP.

Please contact your system administrator for further information.

Value	**Description**	**System Default**
Status	Shows the service status.	Service not running
Mode	• SMTP Proxy: eMails are sent via the system's SMTP Proxy. • Disable SMTP: users are not allowed to send eMails. • Direct SMTP: eMails are sent directly.	SMTP Proxy
SMTP Relayhost	E.g. email.aon.at	
SMTP Authentication	If your ISP requires SMTP Authentication, please activate checkbox and enter Username/Password.	

Public IP

Public IP configuration.

	Requires minimum one public ip range and special routing configurations from ISP.
	'Office-LAN' Proxy ARP allows you to share the same public IP subnet on the 'Office-LAN' and 'Surf-LAN' interface.

Value	**Description**	**System Default**
Status	Shows the service status.	Deactivated
Name	Name and/or description of public ip address pool.	
Start IP Address	Public IP Address range start (e.g.: 192.0.2.1 - hint: omit network address!).	
End IP Address	Public IP Address range end (e.g.: 192.0.2.5).	
Subnet based	Subnet based is recommended. If unchecked clients will get host route to gateway.	
Subnet Mask	Subnet mask of IP Address pool (e.g.: 255.255.255.248).	
Default Gateway	Default Gateway IP Address (e.g.: 192.0.2.6).	
Activate	Set this public ip range active.	

3.3.3 Ticket

Change the settings of the system to meet your requirements.

	The settings should be made by your IT partner as part of the installation process. To make changes, please follow the instructions of your system administrator.

Value	**Description**	**System Default**
Prefix	Displays the username on the 'Surfticket' together with the automated ticket numbering (e.g. ticket1, ticket2).	ticket
Password Length	Defines the length of passwords for 'Surftickets'.	5
Expiration Period	Defines the days a user can consume the time credit (e.g. 365 days).	365
Max Idle Time	Time span in minutes after an inactive session (e.g. no network traffic) is automatically logged off.	20
eMail Statistics to	eMail addresses (separated by a comma) to which statistics are to be sent monthly (common CSV file format).	
Session Limit	Defines the download volume in megabyte a user can consume per session (e.g. 50 MB).	200
Ticket Limit	Defines the download volume in megabyte a user can consume for the entire ticket (e.g. 100 MB).	200

Max Download Bandwidth	Defines the default maximum download bandwidth for 'Surftickets'.	200
Max Upload Bandwidth	Defines the default maximum upload bandwidth for 'Surftickets'.	200

Mandatory Fields

Choose or define fields that ar mandatory when creating a 'Surfticket' within WebAdmin interface.

Data Collector

The Data Collector allows to define additional user input fields (email, name, mobile number etc.) the user has to fill out at login. The Data Collector templates can then be assigned to ticket templates.

Value	**Description**
New	Click to create a new data collector template.
Save	Click to save all created data collector templates.
Name	Enter a proper name for the data collector template.
Single Device Template (Max Devices = 1)	• Disabled: Disables the data collector template if used with a single device ticket template. • First Login: The user has to enter the additional data only at first login. • Every Login: The user has to enter the additional data at every login.
Multi Device Template (Max Devices > 1)	• Disabled: Disables the data collector template if used with a multi device ticket template. • First Login on any device: The user has to enter the additional data only at first login on ANY device. • First Login on each device: The user has to enter the additional data at first login on EACH device. • Every Login: The user has to enter the additional data at every login.
User Input 1-9	Select additional data you want the user to enter at login.

VAT

Value	**Description**	**System Default**
TOTAL Name	Name of total sum on the 'Surfticket'.	TOTAL
VAT Description	VAT description on the 'Surfticket' (e.g. Price includes VAT).	Amount received.

Value	**Description**	**System Default**
Price includes VAT	Defines if the ticket price includes VAT.	Active
VAT Name	Name of VAT on the 'Surfticket'.	VAT
VAT Rate	VAT rate on the 'Surfticket'.	20
NET Name	Name of net sum on the 'Surfticket'.	NET

Invoice

Value	**Description**	**System Default**
Invoice active	Defines if an invoice number should be displayed on the 'Surfticket'.	Inactive
Invoice Description	Name of invoice on the 'Surfticket'.	Invoice
Invoice Prefix	Displays the invoice number on the 'Surfticket' together with the automated invoice numbering (e.g. INV1, INV2).	INV
Invoice number value	Displays the invoice number on the 'Surfticket' together with the invoice prefix (e.g. INV1, INV2); you can set the counter at any time (e.g. 100).	

Logo

The logo will appear on top of the 'Surfticket'.

Ticket Template

Define the 'Surfticket' printout design individually for all languages.

3.3.4 WebAdmin

Change the settings of the system to meet your requirements.

The settings should be made by your IT partner as part of the installation process. To make changes, please follow the instructions of your system administrator.

Value	**Description**
Logon Session expires	Time span in minutes after an inactive session (e.g. no network traffic) is automatically logged off.
Date Format	Choose your desired format.
CSV Separator	Defines which character is used as CSV separator.
Records per page	Defines how many records will be displayed per page when using search functions.
Ticket Format	Defines print format for 'WebAdmin' generated Tickets.

Network Check	Checks your DNS settings and displays an error if the used DNS server is not reachable or has the same IP Address as the used default gateway.
Default Language	If no cookie is set and the browser language is not supported, this language will be preselected at the 'WebAdmin' logon page.
Number Format	Choose your desired format.
Modify 'hosts' File	If your system is Windows-based, you can map the IP Address to the 'WebAdmin' to a special host name by downloading and executing this file. So you can avoid the security alert when accessing the 'WebAdmin'.
Print Note	Print predefined notes on tickets.

3.3.5 License

Ensure that your system has the latest enhancements. If your Online Update Subscription has expired, we would strongly recommend extending it.

It includes:

- Security Updates
- Minor and Major Releases
- Web Filter Lists for Advanced Web Filter
- Latest Security Certificate for 'Surf-LAN' (https)

The settings should be made by your IT partner as part of the installation process. To make changes, please follow the instructions of your system administrator.

Value	**Description**
Status	Shows if your system is licensed.
Online Update Subscription	System can receive Online Updates until the date specified.
Registration Date.	
Current Version.	
Registration MAC	License is bound on this network card (MAC Address).
Registration Number.	
Registration Password.	
User Limit	Maximum concurrent users who can connect to the Internet within the 'Surf-LAN'.
License Key.	
Modules	Shows available modules and their license status.

Registration

To license your system select a registerable network card (MAC address) and enter your Registration Number and Registration Password as shown on your certificate.

Also the Company Name, Location and Administrator Email Address is required for system notifications.

3.3.6 Data Retention

Allows you to automatically delete or anonymize logging and accounting data after a defined retention period.

You will need to comply with your national legal regulations.

3.3.7 Central Services

Used to permanently connect your system to your assigned 'Central Services' server.

The usage requires a valid definition on your assigned 'Central Services' server. Ask your system administrator for further information.

Value	**Description**
Central Server	Full qualified host name or IP Address of your assigned 'Central Services' server.
Service	Activate to start 'Central Server' service.
Remote Access	Activate to get remote access via 'Central Server'.

3.4 System

3.4.1 Services

The services allow you to check the status of the system at any time and to shutdown or to restart the system.

Service running	Service not running	Service not configured

Wherever possible do not switch off the system using the power switch. Use the System/Shutdown function.

	If services are set to red, try to rectify the error by restarting the service.

3.4.2 Manage User

Overview of all created 'WebAdmin' users.

	Please note that Username and Password are case sensitive.
	Change passwords from time to time and keep these in a safe place away from unauthorised access.
	For security reasons, a user must have administrator rights to modify all values.

Value	**Description**
Username	Enter a username.
Password	Enter a password for the user.
Real Name	Enter the real name of the user (optional).
eMail	Enter the email address of the user (optional).
Active	If activated, the user is active and can be used.
Administrator	• Tickets/Create: edit Session Limit, Ticket Limit, Ticket Price. • Tickets/Manage: revoke Used Tickets; display Connection Tracking (if activated). • Tickets/Bulk: edit Session Limit, Ticket Limit, Ticket Price; delete CSV files. • System/Services: restart all services. • System/Manage User: edit Administrator and Active; edit users with administrator rights; see all services. • System/Backup: restore the system. • My Account: edit User Information.
Copy Permissions from	You can copy the rights for services from a existing user.

User Groups

Create user groups and assign certain rights to them. Individual users can then be added to a user group. The user group is necessary to use the ”External Authentication” for WebAdmin login and to enable certain ticket templates only for certain user groups. (E.g. receptionist can only create flat rate 1 day tickets because of the user group he is assigned to)

Value	**Description**
Group Name	Enter a name for the user group.
Description	Enter a description for the user group.
Active	Activate the user group.
Administrator	• Tickets/Create: edit Session Limit, Ticket Limit, Ticket Price. • Tickets/Manage: revoke Used Tickets; display Connection Tracking (if activated). • Tickets/Bulk: edit Session Limit, Ticket Limit, Ticket Price; delete CSV files. • System/Services: restart all services. • System/Manage User: edit Administrator and Active; edit users with administrator rights; see all services. • System/Backup: restore the system. • My Account: edit User Information.
Copy Permissions from	You can copy the permissions from an existing user or user group.

3.4.3 Online Update

Ensure that your system has the latest enhancements. If your Online Update Subscription has expired, we would strongly recommend extending it.

It includes:

- Security Updates
- Minor and Major Releases
- Web Filter Lists for Advanced Web Filter
- Latest Security Certificate for 'Surf-LAN' (https)

Some updates could lead to the system being restarted. Therefore, wherever possible, run manually updates only when the system is not being used.

Value	**Description**

Online Update Subscription	Your system can receive updates until the date specified.
Automatic Onlineupdate	If updates are available, updates will be automatically downloaded and installed at night.
Current Version	Current version of your system.
Logfile	Shows Online Update log history records.

Updates Available

Overview of the currently available updates. If Automatic Online Update is inactive, you can start the download and installation process manually.

Online Update Status

Shows the status of the current/last Online Update.

3.4.4 Remote Control

Support personnel can gain access to your system. During remote maintenance, always follow the instructions of the support staff. The user data for the remote maintenance (username, password) are provided by support staff.

For your own protection, remote maintenance is only possible for support personnel when it has been started by you. By stopping the service you can abort the connection.

3.4.5 Backup

With this function you are able to backup your system configuration files. Due to the amount of data, Connection Tracking records will not be backuped. With help of this file, your system can be restored with state of the last backup.

It includes:

- Tickets
- Configuration
- Settings
- Logo
- Free to Use
- Design
- License

	You can use the backup tool (for Windows or Linux) to run the backup procedure automatically.
	Before running the restore, please check the compatibility of the backup file and the current system (must be the same version number).
	Please contact your system administrator for further information.

The manual backup will return a backup file for downloading.

Remote Backup

The Backup will be automatically stored on a remote FTP server once a day.

Value	**Description**
Type	Remote Backup server type.
Host	Remote Backup server.
Time	Enter start time of remote backup.
Port	Remote Backup server port.
Username	Remote server login username.
Password	Remote server login password.
Remote Directory	Backup directory on remote server.
Max Generations	Number of backup generations to store.
Manage remote files	Show and manage backup files on remote server.
Timeout	Enter a timeout (seconds) after which the remote backup service will be stopped if no successfull backup could have been created.
Force Passive Connection	Activate to use passive FTP mode.
Connections	Check to include Connection Tracking data to the backup.
HTTP Proxy	Check to include HTTP Proxy data to the backup.

Restore

To restore your system, please upload the required backup file. Currently saved information (settings, user management, logs, etc.) and 'Surftickets' will be deleted.

3.4.6 Tools

Value	**Description**
Ping	A computer network tool used to test whether a particular host is reachable across an IP network.

Value	**Description**
ARP Table	Displays the ARP table of the system.

3.4.7 Notifications

Notifications & Remote Syslog

Activate/Deactivate the ”Notifications & Remote Syslog” module. This module allows you to save the syslog on a remote syslog server and/or send notification Emails to a specific Email address if some critical changes happen to the system.

Remote Syslog

Value	**Description**
Activate	Activate / Deactivate the remote syslog.
Host	IP Address or FQDN of remote syslog server.
Port	Enter the port of your remote syslog server (default is 514).

Notifications & Filter

Value	**Description**
Status	Activate/Deactivate the ”Notifications & Filter” function.
Textfield	Define syslog filter and notifications (see standard examples).
Examples	

SNMP - General

Configure SNMP to monitor the system.

Value	**Description**
Device Name	Enter a name for the device to be monitored. (e.g. Internet for Guests)
Device Description	Enter a description for the device to be monitored.
Device Location	Enter the location of the device.
Device Contact	Add a contact name/number for the device to be monitored.
SNMPv1 read community	Define a community with read rights for SNMPv1.
SNMPv1 write community	Define a community with write rights for SNMPv1.
SNMPv3 read user	Define a user with read rights for SNMPv3.
SNMPv3 write user	Define a user with write rights for SNMPv3.
SNMPv3 read password	Define a password for the SNMPv3 read user.
SNMPv3 write password	Define a password for the SNMPv3 write user.

Value	**Description**
Reachable from:	• Office-LAN: If checked, SNMP is reachable from Office-LAN. • Surf-LAN: If checked, SNMP is reachable from Surf-LAN. • Management-LAN: If checked, SNMP is reachable from Management-LAN.

SNMP - Trap Receiver

Configure the SNMP trap receiver.

Value	**Description**
IP Address/Hostname	Enter IP address/hostname of the trap receiver.
Port	Enter the port for the trap receiver.
Community	Enter the community for the trap receiver.
Description	Enter a description for the trap receiver.
SNMP Version	Select SNMP version for the trap receiver.

3.4.8 Monitoring

Add devices (e.g. Access Points) that should be monitored by the monitoring service. Therefore define different commands (checks) which should be executed frequently (e.g. Ping). To automatically receive an Email whenever the checks has been done, configure the SMTP server in the menu ”Settings/Network” and accept the monitoring state at the ”Notifications & Filter” in the menu ”System/Notifications”.

Please contact your system administrator for further information.

General

Value	**Description**
Sleep between checks	Define for how long the monitoring will go to sleep after all checks for all added devices have been done.

Devices - New Device

Add a new device that should be monitored.

Value	**Description**
Host	Enter the host IP address or FQDN of the device that should be monitored.
Description	Enter a description for this device.

Value	**Description**
Active	Check to activate monitoring for this device.

Devices - Show All

Klick to show more detailled information about the configured checks for the devices.

Devices - Check Now

Performs all entered checks for all devices.

Devices - Edit Devices

Edit the selected device and add/delete different checks.

Value	**Description**
Host	Edit the host IP address or FQDN of the device that should be monitored.
Description	Edit the description for this device.
Active	Check to activate monitoring for this device.
Checks	Add specific commands (TCP, HTTP, HTTPS, PING, SSH) that should be executed in order to receive status information about the selected device.

3.5 Security

3.5.1 General

Value	**Description**	**System Default**
Client/Client Protection	Activate to ensure that devices within the 'Surf-LAN' cannot see themselves (only visible for normal system mode).	Active
DNS tunneling Protection	Activate to detect and block DNS tunneling of offline clients.	Active

Logon

Value	**Description**	**System Default**
Secure Logon	Activate to logon via 'https' at the customer logon page.	Active

IEEE 802.1X Authentication - General

Allow IEEE 802.1X authenticator connections from different interfaces.

Value	**Description**
Office-LAN	If checked, allow IEEE 802.1X authenticator connections from Office-LAN.

Value	**Description**
Surf-LAN	If checked, allow IEEE 802.1X authenticator connections from Surf-LAN.
Management-LAN	If checked, allow IEEE 802.1X authenticator connections from Management-LAN.

IEEE 802.1X Authentication - IEEE 802.1X Authenticator Clients

Define IEEE 802.1X authenticator clients (e.g. Access Points).

Value	**Description**
Name	Enter a name for the authenticator client.
Secret	Enter a secret for the authenticator client.
IP Range	Enter an IP range for which 802.1X authentication should be available.
Proxy	If present, enter a 802.1X authenticator proxy.
Radius Attributes	Add additional radius attributes. For further information contact your radius administrator.

IEEE 802.1X Authentication - Manual defined Supplicant Devices

Manually define supplicant devices which should be allowed to connect to the 802.1X network without internet access.

Value	**Description**
Username	Define a username for the supplicant device.
Password	Define a password for the supplicant device.
MAC Address	Enter the MAC address of the supplicant device (optional).
Active	Activate the defined supplicant device.
Radius Attributes	Add additional radius attributes. For further information contact your radius administrator.

3.5.2 Simple Web Filter

Enter any number of websites to block (line by line). Don't bother with the http:// or the www.

3.5.3 Advanced Web Filter

It is possible to restrict websites or download files for guests.

With low-performance computers or high-volume usage, the resource-intensive service can slow down system performance.

	More precise explanations of the setting options and further examples can be found in each category in English (# at the beginning of a line refers to the description text).
	Please contact your system administrator for further information.

Quick Mode

Select from predefined groups of blocked domains and URLs.

	Groups (e.g. Adult, Weapons, etc.) for blocked domains and URLs will be updated by the Online Update.

HTTPS Connections

Value	**Description**
Force HTTPS connections via Content Filter	If active, clients have to use auto-proxy-settings, otherwise direct connections (via NAT) to any HTTPS webserver will be blocked. If inactive, any HTTPS webserver cannot be controlled.

Blocked Domains / URLs

	Groups (e.g. Adult, Weapons, etc.) for blocked domains and URLs will be updated with the Online Update.

Value	**Description**
Blocked Domains	To block top-level domains (.com), domains (e.g. website.com) or subdomains (e.g. support.website.com).
Blocked URLs	To block several URLs within a domain (e.g. website.com/de or website.com/en).

Blocked Downloads

Value	**Description**
Blocked Fileextensions	Filename extension is a suffix to the name of a computer file applied to show its format (e.g. .exe).
Blocked Mime-Types	Metadata about the file format of the data contained (e.g. application/gif for gif format).

Wordlists

Value	**Description**

Value	**Description**
Blocked Words	Websites are blocked if words appear in them that are either contained in predefined groups (e.g. gambling) or have been entered manually.
Exceptions	Disables the word block imposed in Blocked Words.
Use heuristics to block	Websites are blocked when the block threshold for the activated groups of words and for lists of words entered manually has been exceeded.
Threshold for heuristics	Defines the block threshold for Use heuristics to block.

Exceptions (white/grey listing)

Enter any IP address within the 'Surf-LAN', domain or URL which will not be filtered.

Value	**Description**
Whitelisting	Overrules all blocking rules.
Greylisting	Overrules just entries in Blocked Domains and Blocked URLs.

3.5.4 Routes

Define special IP routes for 'Office-LAN', 'Management-LAN' and 'Surf-LAN'.

	The settings should be made by your IT partner as part of the installation process. To make changes, please follow the instructions of your system administrator.
	Please contact your system administrator for further information.

Routes - Editor

Create, edit or delete certain IP routes for both 'Office-LAN' and 'Management-LAN'.

Value	**Description**
Firewall Protection	Check to enable firewall protection for the selected network.
Action	• Activate selected route. • Edit selected route. • Delete selected route.

Routes - New Route

Create new IP routes.

Value	**Description**
Destination Address	IP Address of the destination device or network.

Value	**Description**
Subnet Mask	Subnet Mask for the destination network.
Gateway	IP Address of the next gateway.
Firewall Protection	Protects the 'Office-LAN' / 'Management-LAN' from the 'Surf-LAN' - firewall allows no connection.
Network Interface	Select the network interface for the new route.
Extended Routing active	Activate/deactivate the extended routing settings for this route.
Map to room number (extended routing)	Create a fixed route to room number mapping (only valid, if connected to a property management system).
Logon Mode (extended routing)	• Ticket based: The user has to buy a ticket via PMS, SMS, Email etc. in order to be able to logon. • Autologon / no charge: The user gets logged on automatically without entering any data. Each user gets the defined bandwith limits. • Autologon / no charge / deny roaming: The user gets logged on automatically without entering any data. Each user gets the defined bandwith limits. Ticket is only valid in this specific VLAN. • Autologon / no charge / shared bandwidth: The user gets logged on automatically without entering any data. All users in this Vlan share the defined bandwith limits. • Autologon / no charge / shared bandwidth / deny roaming: The user gets logged on automatically without entering any data. All users in this Vlan share the defined bandwith limits. Ticket is only valid in this specific VLAN.
Redirect before logon (extended routing)	Used to redirect clients to specific information website before valid logon. Only valid, if per ”VLAN and routing redirect before logon” is activated and custom ”Redirect before logon” websites are defined.
Fixed Bandwidth (extended routing)	If logon mode ”Autologon / no charge / shared bandwidth” is active: activate to set the configured up - and download bandwidth as fixed bandwidth for this route.
Max Download Bandwidth (extended routing)	If logon mode ”Autologon / no charge” is active: defines the maximum download bandwidth for this route.
Max Upload Bandwidth (extended routing)	If logon mode ”Autologon / no charge” is active: defines the maximum upload bandwidth for this route.
Bypass Web Filter (extended routing)	If web filter is activated, check to bypass web filter for this route. All users within the destination network have unrestricted internet access.
Session Limit (extended routing)	If logon mode ”Autologon / no charge” is active: define the volume in megabyte one station can consume per session.

Value	**Description**
Allow Free Logon (extended routing)	• No: Do not allow free logon for this route. • Yes: Allow free logon for this route. • Yes but PMS authentication required: Allow free logon with PMS authentication for this route. If ”Limit to VLAN” is activated at the free logon configuration in the menu ”Tickets/Templates” the free logon template can be activated for each route separately.

Routes - Extended Routing

Activate to show enhanced options for 'Surf-LAN' routing.

Value	**Description**
Per VLAN and routing redirect before logon	Activate to redirect to different websites before logon. For each route a separate website can be defined.
Prefer routing match	If both VLAN's and Extended Routing is active, settings made for extended routing will always be preferred.

Routes - Show Routes

Shows all currently active routes.

3.5.5 Port Filter

Define ports to be blocked for 'Surf-LAN'.

Please contact your system administrator for further information.

Value	**Description**
Type	Description of port type.
Name	Description of blocked port range.
Protocol	UDP and/or TCP protocol is blocked - depending on service.
Port Range	Block ports from/to.
Edit	Edit the selected port filter.
Delete	Edit the selected port filter.

3.5.6 Proxy

Define additional proxy ports for 'Surf-LAN' the https proxy server should listen to.

	Please note, that on all defined ports no other Internet application service can run.
	Please contact your system administrator for further information.

Value	**Description**
Name	Description of proxy port (e.g. company proxy).
Proxy Port	Enter proxy port to listen for queries.
Edit	Edit the selected proxy rule.
Delete	Delete the selected proxy rule.

Upstream Proxy

Define an upstream proxy and port of a parent proxy.

3.5.7 MAC Filter

Filter devices by their MAC address. Devices added to the MAC Filter do not get any logon page and can not connect to the system.

Clients online

Shows the clients that are currently online.

New device

Add a new device to the MAC Filter. Enter MAC Address, name and description to filter this device.

3.5.8 VLAN

Define VLANs for 'Surf-LAN'. This is used for room / port isolation with VLAN enabled switches.

	If enabled all network frames must include a VLAN tag. Untagged frames will be ignored.
	Please contact your system administrator for further information.

Do not define VLAN ID 1. Most switches use this as default VLAN and for management and can be operated only untagged.

Add / Edit VLAN

Value	**Description**
VLAN ID	Number of VLAN ID. All defined VLAN IDs must be defined 'tagged' on your switch trunk port, where your systems 'Surf-LAN' interface is connected to.
Description	Some detail information about location or usage.
Map to room number	Create a fixed VLAN to room number mapping (only valid, if connected to a property management system).
Logon Mode	• Ticket based: The user has to buy a ticket via PMS, SMS, Email etc. in order to be able to logon. • Autologon / no charge: The user gets logged on automatically without entering any data. Each user gets the defined bandwith limits. • Autologon / no charge / deny roaming: The user gets logged on automatically without entering any data. Each user gets the defined bandwith limits. Ticket is only valid in this specific VLAN. • Autologon / no charge / shared bandwidth: The user gets logged on automatically without entering any data. All users in this Vlan share the defined bandwith limits. • Autologon / no charge / shared bandwidth / deny roaming: The user gets logged on automatically without entering any data. All users in this Vlan share the defined bandwith limits. Ticket is only valid in this specific VLAN. • Show only room number: If connected to a PMS, the room number is displayed at the PMS logon. • Semiautomatic logon: If connected to a PMS, the user can select a ticket without entering his user data.
Session Limit	If VLAN ”Autologon / no charge” is active: defines the volume in megabyte one station can consume per session.
Max Download Bandwidth	If VLAN ”Autologon / no charge” is active: defines the maximum download bandwidth for this VLAN.
Max Upload Bandwidth	If VLAN ”Autologon / no charge” is active: defines the maximum upload bandwidth for this VLAN.
Fixed Bandwidth	If VLAN ”Autologon / no charge / shared bandwidth” is active: activate to set the configured up - and download bandwidth as fixed bandwidth for this VLAN.

Value	**Description**
Redirect before logon	Used to redirect clients to specific information website before valid logon. Only valid, if per ”VLAN Redirect before logon” is activated and custom ”Redirect before logon” websites are defined.
Bypass Web Filter	If web filter is activated, check to bypass web filter for this VLAN. All users within this VLAN have unrestricted internet access.
Allow Free Logon	• No: Do not allow free logon for this VLAN. • Yes: Allow free logon for this VLAN. • Yes but PMS authentication required: Allow free logon with PMS authentication for this VLAN. If ”Limit to VLAN” is activated at the free logon configuration in the menu ”Tickets/Templates” the free logon template can be activated for each VLAN separately.
Active	Enable or disable this VLAN.
Action	Enable, disable, edit or delete current selected entry.

Upload VLAN List

Allows you to upload a text file with all VLAN definitions.

Define one VLAN per line. Valid field delimitors are: ';' and ','

File format description

Field #	**Field name**	**Value type (range)**	**Field description**
1	VLAN ID	numeric (1 - 4095)	Number of VLAN ID (do not use ID 1, because many switches operates VLAN ID 1 only untagged).
2	Description	string	Some detail information about location or usage.
3	Active	numeric (0 - 1)	0 = VLAN disabled; 1 = VLAN enabled
4	Map to room number	alphanumeric	Define room number without leading zero. Type '=' to use VLAN ID as room number.

Field #	**Field name**	**Value type (range)**	**Field description**
5	Number of URL for ”Redirect before logon”.	numeric (1 - 20)	Used to redirect clients to specific information website before valid logon. Only valid, if per ”VLAN Redirect before logon” is activated and custom ”Redirect before logon” websites are defined.
6	Logon Mode	numeric (0 - 4)	0 = Ticket based; 1 = Show only room number; 2 = Semiautomatic login; 3 = Autologon / no charge; 4 = Autologon / no charge / deny roaming;
7	Max MB limit per session	numeric (0 - 999999)	0 = use system defaults as defined in menu ”Settings / Ticket”
8	Max Download Bandwidth	numeric (0 = use current system maximum)	Define download bandwidth in kBit/s
9	Max Upload Bandwidth	numeric (0 = use current system maximum)	Define upload bandwidth in kBit/s
10	Bypass Web Filter	numeric (0 - 1)	0 = disabled; 1 = enabled
11	Show Free Logon	numeric (0 - 2)	0 = disabled, 1 = enabled, 2 = enabled with PMS logon required

File format example

Line #	**Example entry**
1	2;Wireless Lobby;1;;1;0;;;;;;
2	3;Surfterminal Lobby;1;;1;3;5000;2048;1024;1;1
3	200;Room A200;1;A200;2;1;;;;;;
4	300;VIP room 300;1;=;4;3;5000;4096;2048;;1
n	VLANIDn;DESCRn;ACTIVEn;ROOMn;URLn;LOGONn;MAXMBn;BWDOWNn;BWUPn;WEBFBYPn;FREELGNn

3.5.9 Port Forwarding (DNAT)

Define port forwardings from 'Office-LAN' to 'Surf-LAN'. This is used for accessing devices located inside 'Surf-LAN' by devices from outside the 'Surf-LAN' (e.g. 'Office-LAN').

Please contact your system administrator for further information.

Add / Edit DNAT Rule

Value	**Description**
Allowed source IP Address/Network	Allow access from specific source address or network. E.g.: allow all hosts from 192.168.10.0/24 ip range to access a specific device from 'Surf-LAN'.
Local Port	Define the local port for outside access to the device (valid values: from 9000 to 65000).
Destination IP Address	Define the IP Address of the device which is located on the 'Surf-LAN' side.
Destination Port	Define the IP Port of the device which is located on the 'Surf-LAN' side.
Protocol	IP based protocols 'tcp' and 'udp' are supported.
Description	A short description about the rule.
Interface	Source interface of the rule.
Activate	Enable or disable the DNAT rule.
Monitoring	Destination IP port is monitored.
Action	Enable, disable, edit or delete current selected entry.

Example

Accesspoint (AP) in 'Surf-LAN' has IP 172.30.3.250 and has a web based management interface listening on port 80. You want to manage this AP form an 'Office-LAN' client with IP 192.168.10.20. 'Internet for Guests Server' has IP 192.168.10.100.

Value	**Example entry**
Allowed source IP Address/Network	192.168.10.20/32
Local Port	10080
Destination IP Address	172.30.3.250
Destination Port	80
Protocol	tcp
Description	Remote Management AP1

Now you can access the AP web management interface by using http://192.168.10.100:10080 from client 192.168.10.20.

Use 192.168.10.0/24 as ”Allowed source IP Address/Network” to allow access from the whole 192.168.10.0 subnet.

3.6 Modules

3.6.1 Autologon Devices

Computers can automatically be activated in the 'Surf-LAN' to access the web (surf terminals, workshop laptops, etc). This can be done by either selecting a device currently available in the 'Surf-LAN' or by manually entering the IP/MAC Address.

Please note that each autologon device counts as one license use.

Value	**Description**
Activate/Deactivate	Activate or deactivate device.
Edit	Edit selected autologon device.
Delete	Delete selected autologon device.

Clients Online

IP/MAC Address of currently connected devices to activate per click.

New Device

Value	**Description**
IP Address	IP Address of the new autologon device.
MAC Address	MAC Address of the new autologon device.
Max Download Bandwidth	Defines the maximum download bandwidth for the new autologon device.
Max Upload Bandwidth	Defines the maximum upload bandwidth for the new autologon device.
Activate	Check to activate the new autologon device.
Fixed Bandwidth	Check to use the configured bandwidth as fixed bandwidth for this autologon device.
New DHCP Static Lease	Adds a static IP-Address for the autologon device (recommended).
Name	Enter a name for the new autologon device.
Description	Enter a description for the new autologon device.
Session Limit	Define the session limit of the new autologon device.
Ticket Limit	Define a ticket limit for the new autologon device.

Value	**Description**
PMS Authentication	Check to force pms authentication for the new autologon device.

Upload Device List

Allows you to upload a text file with all autologon devices.

Define one autologon device per line. Valid field delimitor is: ';'

File format description.

Field #	**Field name**	**Value type (range)**	**Field description**
1	IP Address	string	Enter the IP Address of the autologon device.
2	MAC Address	string	Enter the MAC Address of the autologon device.
3	Name	string	Enter a name for the autologon device.
4	Description	string	Enter a description for the autologon device.
5	Active	numeric (0 - 1)	0 = disabled; 1 = enabled
6	Max Download Bandwidth	numeric (0 = system default)	Define download bandwidth in kBit/s.
7	Max Upload Bandwidth	numeric (0 = system default)	Define upload bandwidth in kBit/s.
8	Session Limit	numeric (0 = system default)	Define a session limit for the autologon device. When reaching the session limit, the device will get logged off for a short amount of time and then automatically goes back online.
9	Ticket Limit	numeric (0 = system default)	Define a ticket limit for the autologon device. When reaching the ticket limit, a new autologon ticket will be created automatically.
10	PMS Authentication	numeric (0 - 1)	0 = disabled; 1 = enabled

File format example.

Line #	**Example entry**
1	172.30.0.25;00:01:02:03:04:05;AccessPoint1;;1;2048;2048;500;5000;0
2	172.30.0.26;00:01:02:03:04:06;AccessPoint2;;;;;;;
3	172.30.0.27;00:01:02:03:04:07;Surfterminal;;1;521;512;500;5000;0
n	IP-ADDRESSn;MAC-ADDRESSn;NAMEn;DESCRn;ACTIVEn;BWDOWNn;BWUPn;SESSLIMITn;TICKETLIMITn;PMSAUTHn

3.6.2 PMS

'PMS' ('Property Management System' - front office systems for hotels, cruisers, etc.) allows the guest to generate a 'Surfticket' him/herself at the customer logon page. The amount due is added directly to the bill for the room. The settings are defined by your 'PMS' IT partner.

	Your system may not support this feature.
	To connect the system with 'PMS', you also need to have a module from the respective manufacturer.
	The settings should be made by your IT partner as part of the installation process. To make changes, please follow the instructions of your system administrator.
	When you use the 'PMS' module do not forget to enable at least one ticket template for 'PMS' use!

Value	**Description**
Type	Select PMS type.
Character set	PMS server character set.
IP Address	IP Address of PMS server.
Port	Port on which PMS server is listening for connections.
Authentication	Select values that are used for PMS user authentication.
No charge mode	When checked, users will get free internet access after successful PMS authentication.
Skip zero posting	Check if free ticket templates are provided for the PMS authentication.
VIP / Membership	Configure VIP groups to offer different tickets based on the VIP group the user is assigned to (only available when selected PMS type supports VIP group membership).

Allow multiple VIP Groups	Check to allow to assign multiple VIP groups to a user (only available when selected PMS type supports VIP group membership).
VIP Group Delimiter	Select the delimiter which is used to separate multiple VIP groups (only available when selected PMS type supports VIP group membership).
PMS Caching	Check to activate PMS Caching.
Caching Hours	Define for how long a user can still login after checkout (valid ticket required).
Caption	Define custom captions on customer logon page.

Demo PMS

If PMS type is set to 'Demo PMS' you can find the login information for the demo users.

PMS Blacklist

Define room numbers which do not allow guests to logon via PMS interface.

Multimedia Service

The 'Multimedia Service' module allows you to connect to various IP-TV-Systems. The settings are defined by your IT partner.

	Your system may not support this feature.
	The settings should be made by your IT partner as part of the installation process. To make changes, please follow the instructions of your system administrator.
	When you use the Multimedia module do not forget to enable at least one ticket template for Multimedia use!

Value	**Description**
Type	Select Multimedia Interface type.
Role	Select whether the HSC HotSpot should act as TCP/IP server or TCP/IP client.
Server	If used as server, the IP-Address of the HSC HotSpot is entered automatically. If used as client, the IP-Address of the multimedia server must be entered.
Port	IP Port which shall be used for this connection.
Shared Secret	Setting of the password for the connection establishment between HSC HotSpot and Multimedia server. On both sides the same password must be defined.

Messaging: SMS

The 'Messaging: SMS' module allows guests to register themselves for a 'Surfticket' at the customer logon page by providing the mobile number. The settings are defined by your IT partner.

	Your system may not support this feature.
	To connect the system with 'Messaging: SMS', you also need to have a SMS provider to connect to.
	The settings should be made by your IT partner as part of the installation process. To make changes, please follow the instructions of your system administrator.
	When you use the 'Messaging: SMS' module do not forget to enable at least one ticket template for 'Messaging: SMS' use!

Value	**Description**
Hide Login	Activate to hide the SMS login button at the client logon page while the module stays enabled. Used for Online Payment with ticket delivery via SMS.
Type	Select SMS provider.
Server	Enter the server address of your SMS provider.
Username and Password	Authentication data of your SMS provider.
Message	This message will be send to the user after successful registration.
Method	Select the method which is specified by your SMS provider. (only available when 'Generic via HTTP' is selected as type)
Request	Configure the request which is specified by your SMS provider. (only available when 'Generic via HTTP' is selected as type)
Return Validation	Validate whether the SMS has been successfully sent or not. E.g. Return validation is 'status:”1”'. If the return string does not contain the entered return validation, we assume an error occurred and show an error message at the customer logon site.
Max. SMS/total	Total number of SMS send per day/week/month/year (depending upon settings).
Max. SMS/user	Total number of SMS send per user (depending upon settings).
Mandatory field	Select a mandatory field the user has to enter in order to generate a 'Surfticket'.

Instruction	Depending upon selected mandatory field, a short guidance for the user can be entered.
Prefix	International country code preselection.
Filter	Block or allow certain phone numbers and range of phone numbers.
User Input 1-9	Optional: define additional data fields, which the user must enter to generate a 'Surfticket'.
Test SMS	Send a test SMS to check current configuration.

Messaging: Email

The 'Messaging: Email' module allows guests to register themselves for a 'Surfticket' at the customer logon page by providing a valid email address. The settings are defined by your IT partner.

	Your system may not support this feature.
	Usage of 'Messaging: Email' requires valid email provider settings. See menu ”Settings/Network/SMTP Server” for configuration.
	The settings should be made by your IT partner as part of the installation process. To make changes, please follow the instructions of your system administrator.
	When you use the 'Messaging: Email' module do not forget to enable at least one ticket template for 'Messaging: Email' use!

Value	**Description**
Hide Login	Activate to hide the email login button at the client logon page while the module stays enabled. Used for Online Payment with ticket delivery via email.
Sender	Sender email address.
Subject	Subject of the email which is send to the customer after registration.
Message	Message of the email which is send to the customer after registration.
Max. Emails total	Total number of emails send per day/week/month/year (depending upon settings).
Max. Emails/user	Maximum number of emails per user per interval.
Activation time slot	Time in minutes for activation. Therefore the customer has to confirm the generated 'Surfticket' by clicking on an activation link in the email that has been send to him.

Suppress Attachments	If activated, only your defined text message will be sent. No attachment will be added.
Mandatory field	Select values the user has to enter in order to generate a 'Surfticket'.
Filter	Block or allow certain email addresses or domains.
User Input 1-9	Optional: define additional data fields, which the user must enter to generate a 'Surfticket'.
Testmail	Send test email to check the current configuration.

Social Login: General

Configure general settings for the Social login module.

Value	**Description**
Hide Ticket Logon	Activate to hide the ticket logon dialog.
Display Social Login first	Activate to switch positions of ticket logon and social login buttons.

Social Login: 'Facebook'

The Social Login: 'Facebook' module allows users to use their existing 'Facebook' account to authenticate. The settings are defined by your IT partner.

	To connect the system with Social Login: 'Facebook', you need to create your own 'Facebook' app.
	The settings should be made by your IT partner as part of the installation process. To make changes, please follow the instructions of your system administrator.
	When you use the Social Login: 'Facebook' module do not forget to enable at least one ticket template for Social Login use!

Value	**Description**
Name	Enter a name for the 'Facebook' connector.
App ID	Enter the app ID of your 'Facebook' app you created.
App Secret	The app secret must match with the secret in your 'Facebook' app your created.
Display	Select how to display authentication dialog.
Ticket Template	Ticket template assigned to successfully authenticated users.
Activation time slot	Time slot in minutes within user has to logon, using his social account.
Advanced	Configure advanced options.

Callback URL	URL of the client logon page. If you use a custom SSL certificat for the client logon page, you need to adapt the Callback URL to your custom host - and domain name.
Access Token URL	Do not change unless 'Facebook' changes its API (default recommended).
Authorize URL	Do not change unless 'Facebook' changes its API (default recommended).
Post on Wall URL	Do not change unless 'Facebook' changes its API (default recommended).
Userinfo URL	Do not change unless 'Facebook' changes its API (default recommended).
Post on Wall	Check to post messages, links and place to the users profile page.
Message	Post a message to the users profile page.
Place	Enter the link of your 'Facebook' Place (example: https://www.facebook.com/myplace). The appropriate Place ID is detected automatically.
Link	Post a link to the users profile page.

Social Login: 'Google'

The Social Login: 'Google' module allows users to use their existing 'Google' account to authenticate. The settings are defined by your IT partner.

	To connect the system with Social Login: 'Google', you need to create your own 'Google' app.
	The settings should be made by your IT partner as part of the installation process. To make changes, please follow the instructions of your system administrator.
	When you use the Social Login: 'Google' module do not forget to enable at least one ticket template for Social Login use!

Value	**Description**
Name	Enter a name for the 'Google' connector.
Client ID	Enter the client ID of your 'Google' app you created.
Client Secret	The client secret must match with the secret in your 'Google' app your created.
Display	Select how to display authentication dialog.
Ticket Template	Ticket template assigned to successfully authenticated users.
Activation time slot	Time slot in minutes within user has to logon, using his social account.

Advanced	Check to configure advanced options.
Callback URL	URL of the client logon page. If you use a custom SSL certificat for the client logon page, you need to adapt the Callback URL to your custom host - and domain name.
Access Token URL	Do not change unless 'Google' changes its API (default recommended).
Authorize URL	Do not change unless 'Google' changes its API (default recommended).
Userinfo URL	Do not change unless 'Google' changes its API (default recommended).

Social Login: 'Windows Live'

The Social Login: 'Windows Live' module allows users to use their existing 'Windows Live' account to authenticate. The settings are defined by your IT partner.

	To connect the system with Social Login: 'Windows Live', you need to create your own 'Windows Live' app.
	The settings should be made by your IT partner as part of the installation process. To make changes, please follow the instructions of your system administrator.
	When you use the Social Login: 'Windows Live' module do not forget to enable at least one ticket template for Social Login use!

Value	**Description**
Name	Enter a name for the 'Windows Live' connector.
Client ID	Enter the client ID of your 'Windows Live' app you created.
Client Secret	The client secret must match with the secret in your 'Windows Live' app your created.
Display	Select how to display authentication dialog.
Ticket Template	Ticket template assigned to successfully authenticated users.
Activation time slot	Time slot in minutes within user has to logon, using his social account.
Advanced	Check to configure advanced options.
Redirect domain	URL of the client logon page. If you use a custom SSL certificat for the client logon page, you need to adapt the Redirect domain to your custom host - and domain name.
Access Token URL	Do not change unless 'Windows Live' changes its API (default recommended).
Authorize URL	Do not change unless 'Windows Live' changes its API (default recommended).

Userinfo URL	Do not change unless 'Windows Live' changes its API (default recommended).

3.6.3 Authentication

The ”Authentication” module allows you to authenticate users against different backends.

	A valid license with 'External Authentication' is required to use this module (except ”Local Database”).
	Supported backends: Local Database, Active Directory, LDAP, MSSQL, MySQL, PostgreSQL, Radius and iPass.
	Define and enable at least one ticket template or external user template for 'External Authentication'.

Local Database

When Local Database is selected, users can be defined in menu ”Tickets / Users”.

Active Directory / LDAP

Value	**Description**	**Example**
Backend	Select type of backend.	
Use for WebAdmin	If activated, authentication is used for 'WebAdmin' user login. At least one active user group in the menu 'System / Manage User' is required.	
Name	Define a name for the backend.	
Server	IP Address or FQDN of backend server.	
SSL	Enable SSL encryption (if supported by backend).	
Port	Port where backend server is listening for connections.	
Ticket Template	Ticket template assigned to successful authenticated users.	
Max Users	Maximum number of users that can login simultaneously with same username and password.	

Value	**Description**	**Example**
Shared Limits	• checked: Ticket limits provided by template are shared among multiple users. • unchecked: Every logged in user obtains the ticket limits provided by template.	
Repeat Interval	Ticket will automatically renew after expiration (e.g. ticket limit exceeded).	
Force Account Lookup	Disable local account caching.	
Character set	Backend character set.	
Anonymous Bind	Check for anonymous LDAP bind (not supported by Active Directory).	
Bind DN	The bind DN is the user on the external LDAP server permitted to search the LDAP directory. The role of the bind DN is to query the directory using the LDAP query filter and search base for the DN (distinguished name) for authenticating users.	cn=administrator,cn=Users,dc=domain,dc=com
Password	Password for Bind DN to connect to LDAP server.	
Base DN	The search base (Base DN) tells the server which part of the external directory tree to search.	
User Attribute	Ticket will automatically renew after expiration (e.g. ticket limit exceeded).	ou=Users,dc=domain,dc=com
Group DN (optional)	Search for group membership.	
Access Attribute (optional)	Define attribute of group membership.	memberOf
Username	Username to test authentication.	
Password	Password to test authentication.	

MSSQL / MySQL / PostgreSQL

Value	**Description**
Backend	Select type of backend.
Use for WebAdmin	If activated, authentication is used for 'WebAdmin' user login. At least one active user group in the menu 'System / Manage User' is required.
Name	Define a name for the backend.
Server	IP Address or FQDN of backend server.
Port	Port where backend server is listening for connections.
Ticket Template	Ticket template assigned to successful authenticated users.
Max Users	Maximum number of users that can login simultaneously with same username and password.

Value	**Description**
Shared Limits	• checked: Ticket limits provided by template are shared among multiple users. • unchecked: Every logged in user obtains the ticket limits provided by template.
Repeat Interval	Ticket will automatically renew after expiration (e.g. ticket limit exceeded).
Force Account Lookup	Disable local account caching.
Database	Name of database to connect to.
Character set	Backend character set.
Username	Username for database connection.
Password	Password for database connection.
SQL Login	SQL statement for authentication.
Username	Username to test authentication.
Password	Password to test authentication.

Radius

Value	**Description**
Backend	Select type of backend.
Use for WebAdmin	If activated, authentication is used for 'WebAdmin' user login. At least one active user group in the menu 'System / Manage User' is required.
Name	Define a name for the backend.
Server	IP Address or FQDN of backend server.
Port	Port where backend server is listening for connections.
Shared Secret	Shared secret must match with the shared secret of the backend server.
Radius Accounting	If activated, the server sends accounting informations to the radius accounting server at loggon and logoff events.
Ticket Template	Ticket template assigned to successful authenticated users.
Max Users	Maximum number of users that can login simultaneously with same username and password.
Shared Limits	• checked: Ticket limits provided by template are shared among multiple users. • unchecked: Every logged in user obtains the ticket limits provided by template.
Repeat Interval	Ticket will automatically renew after expiration (e.g. ticket limit exceeded).
Force Account Lookup	Disable local account caching.

Value	**Description**
Username Lowercase	Convert usernames to lowercase.
Username	Username to test authentication.
Password	Password to test authentication.

iPass

For the external authentication via iPass, certain iPass client software is needed. For further information please contact your iPass partner.

Value	**Description**
Backend	Select type of backend.
Name	Define a name for the backend.
Server	IP Address or FQDN of backend server.
Port	Port where backend server is listening for connections.
Shared Secret	Shared secret must match with the shared secret of the backend server.
Radius Accounting	If activated, the server sends accounting informations to the radius accounting server at loggon and logoff events.
NAS - IP - Address	For configuration details, please contact your iPass partner.
NAS - Identifier	For configuration details, please contact your iPass partner.
WISPR Location ID	For configuration details, please contact your iPass partner.
WISPR Location Name	For configuration details, please contact your iPass partner.
Ticket Template	Ticket template assigned to successful authenticated users.
Max Users	Maximum number of users that can login simultaneously with same username and password.
Shared Limits	• checked: Ticket limits provided by template are shared among multiple users. • unchecked: Every login user obtains the ticket limits provided by template.
Repeat Interval	Ticket will automatically renew after expiration (e.g. ticket limit exceeded).
Force Account Lookup	Disable local account caching.
Username	Username to test authentication.
Password	Password to test authentication.

3.6.4 Ticket Printer

If you use a ticket printer that comes with the system you can generate 'Surftickets' at the press of a button. Pressing the Feed button tightens the roll of paper. To print out the 'Surfticket', the Print button may have to be pressed a number of times depending on the ticket type (e.g. to print out ticket type 2, the Print button has to be briefly pressed twice).

You can define each ticket template to be available for the ticket printer in the menu

Tickets/Templates. 'Surftickets' generated by the ticket printer are available in English, German, French, Italian, Dutch, Spanish, Danish and Swedish. Press the Test button to print out a selection of all defined ticket types. You can operate up to 16 devices.

	Your system may not support this feature.
	The settings should be made by your IT partner as part of the installation process. To make changes, please follow the instructions of your system administrator.

Settings

Value	**Description**
Type	Select one of the supported ticket printers.
Location	Enter the location of the ticket printer (e.g. reception).
Language	Select the ticket language for the printer.
Ticket Format	Select the width of the ticket printer paper (80mm / 58mm) (only available for Ticketprinter EPSON TM-T20).
Copy	Prints the 'Surfticket' two times.
Port	Enter the port (e.g. COM1/COM2 or eCOV-100 with IP Address, IP Port and Password).
IP Address	Enter the IP Address of the ticket printer.
IP Port	Enter an IP Port for the ticket printer (usually default port works fine).
Password	Enter a password for the ticket printer.

3.6.5 DHCP

Define DHCP Static Leases for devices in the 'Surf-LAN' and create new DHCP ranges (protected / unprotected) for the 'Surf-LAN'.

	If you create a new subnet within the 'Surf-LAN' (e.g. business corner) enter a valid gateway address for the devices to enable real Plug and Play.
	Please contact your system administrator for further information.

DHCP - Static Leases

Edit selected DHCP Static Lease.

Value	**Description**

Value	**Description**
Action	• Activate / Deactivate selected DHCP Static Lease. • Edit selected DHCP Static Lease. • Delete selected DHCP Static Lease.

DHCP - Clients Online

Shows detailed information (IP/MAC Address, Hostname etc.) of currently connected devices to activate per click.

DHCP - New DHCP Static Lease

Define new DHCP Static Leases for devices in the 'Surf-LAN'.

Value	**Description**
IP Address	Enter a new static IP Address for the device.
Name	Enter a name for the device.
MAC Address	Enter the MAC Address of the device.
Description	Enter a description for the device.
Subnet Mask	Enter the Subnet Mask for the new static IP Address.
Default Gateway	Enter the default gateway for the device.
Activate	Activate Static Lease for the selected device.

DHCP - Dynamic Leases

Shows detailed information (IP/MAC Address, Hostname etc.) of currently used dynamic leases. Individual leases can be deleted.

DHCP - Ranges

Shows detailed information of currently defined DHCP ranges for 'Surf-LAN'.

Value	**Description**
State	Activated / Deactivated.
Type	Protected / Unprotected.
Action	Delete selected DHCP range.

DHCP - New DHCP Range

Define new DHCP ranges (protected / unprotected) for the 'Surf-LAN'.

Value	**Description**
Start IP Address	Enter Start IP Address for new DHCP range.
End IP Address	Enter End IP Address for new DHCP range.
Default Gateway	Enter Default Gateway for new DHCP range.

Value	**Description**
Subnet Mask	Enter Subnet Mask for new DHCP range.
Protected	Check for new protected DHCP range.

DHCP - Advanced Settings

Edit the DHCP Lease Time and set special DHCP configuration settings.

Value	**Description**
Lease Time	Define the DHCP lease time in minutes.

3.6.6 Connection Tracking

Allows you to record IP connections and HTTP Proxy connections (visited websites).

	You have to comply with your national legal regulations when using this feature.
	If you deactivate the module, all data recorded so far will be deleted.
	Please make sure connection tracking is legal for your use!

Value	**Description**
Connections	Recording of all IP connections regardless of protocol.
HTTP Proxy	Recording of all visited websites (HTTP traffic only, no HTTPS traffic).
Delete Tracking data after	Recorded data will be deleted automatically after defined period.

3.6.7 Online Payment

Online payment interface allows the guest to purchase a 'Surfticket' him/herself at the customer logon page. The customer gets charged by the online payment institution. The settings are defined by the online payment service provider.

	To connect the system to your online payment provider you need an account from the respective provider.
	When you use the online payment module do not forget to enable at least one ticket template for online payment use!

Value	**Description**
Online Payment Provider	Select your online payment provider ('PayPal-Sandbox-Test' is for testing only).
Online Payment Provider Homepage	The button links to the homepage of the selected online payment provider.
Username	Enter the username of your API credentials.
Password	Enter the password of your API credentials.
Signature	Enter the signature of your API credentials.
VAT Rate	Enter the VAT rate for online payment tickets.
Display Logo	Show or hide the logo from the selected online payment provider on the customer logon site.

Advanced Notification (SMS and/or Email)

The Advanced Notification allows you to additionally send the ticket details (username, password) via SMS or Email after purchasing a ticket via online payment. The Advanced Notification can only be used when eighter SMS or Email module is activated and configured.

Value	**Description**
SMS	Activate/deactivate the Advanced Notification via SMS message.
Require SMS	If checked, the phone number of the user is required in order to use the online payment. The message with the ticket details above will be send to the users phone.
Email	Activate/deactivate the Advanced Notification via Email message.
Require Email	If checked, the Email address of the user is required in order to use the online payment. The message with the ticket details above will be send to the entered Email address.
Require Email or SMS	If checked, eighter the phone number or the Email address of the user is required in order to use the online payment.
Message	This message will be send to the user after successful registration. Therefore you need a licensed and configured SMS and/or Email module.
Attach Ticket to Email	If checked, the html ticket layout which includes the complete ticket data (max. devices, time credit, ticket limit etc.) will be send as attachment when using Email message.

3.6.8 Plug & Play

Define MAC addresses which are ignored by the Plug & Play engine for devices in the 'Surf-LAN'. This can be useful for set-top boxes which reside in 'Surf-LAN' for example.

Please contact your system administrator for further information.

Plug & Play - Ignored Devices

Shows all devices that are currently ignored by the Plug & Play.

Plug & Play - Clients Online

IP/MAC address of currently connected devices to activate per click.

Plug & Play - New Device

Value	**Description**
MAC Address	Enter the MAC Address of the device.
Description	Enter a description for the device.
Name	Enter a name for the device.

Plug & Play - Upload Device List

Allows you to upload a text file with all devices that should be ignored by the Plug & Play engine.

Define one device per line. Valid field delimitors are: ';' & ','

File format example

Line #	**Example entry**
1	MAC-ADDRESS1; NAME1; DESCRIPTION1
2	MAC-ADDRESS2; NAME2;DESCRIPTION2
3	MAC-ADDRESS3; NAME3;DESCRIPTION3
n	MAC-ADDRESSn; NAMEn;DESCRIPTIONn

Plug & Play - DNS Bypass

In case of an NXDOMAIN DNS response (non existing domain) the DNS answer to the client will not be replaced with the Surf-LAN IP address and the client receives the original DNS response (E.g. avoid timeouts when using directory servers).

Plug & Play - Add Bypass Domain Name

Value	**Description**
Domain Name	Enter a Domain Name to bypass. Only Regex or FQDN allowed.
Description	Enter a description for the bypass Domain Name.

Plug & Play - DNS Redirect

For any DNS request of a defined Domain Name the DNS answer to the client will be the defined IP address (DNS A-Record).

Plug & Play - Add Redirect Domain Name

Value	**Description**
Domain Name	Enter a Domain Name to be replaced.
Description	Enter a description.
IP Address	Enter the IP address for the defined Domain Name.

3.6.9 Application Control - Policies

This allows you to log, reject or shape various network protocols such as P2P filesharing protocols etc. Therefore activate the relevant protocols and select the action which should be used for them (Reject, Bandwidth Shaping, Log only).

Your system may not support this feature.

Value	**Description**
Verbose Logging	Activate, to log all events concerning activated network protocols.
Statistics	Shows all activated protocols with their selected action and the traffic they generate.
Action	• Reject: Packets will be dropped. • Bandwidth Shaping: Traffic will be limited depending on the selected bandwidth group. • Log only: Traffic will be logged only for analyzing Surf-LAN network traffic.

Application Control - Bandwidth Groups

Define different bandwidth groups and assign them to the network protocols which should be bandwidth shaped. The network protocols are only allowed to use the defined bandwidth of the assigned bandwidth group. This allows you to completely block, log or slow down specific traffic in your Surf-LAN environment.

Value	**Description**
Description	Enter a description for the bandwidth group (e.g. P2P-slow).
Download Bandwidth	Select the download bandwidth for the bandwidth group.
Upload Bandwidth	Select the upload bandwidth for the bandwidth group.

3.7 Reporting

3.7.1 Application

Chronological listing of the most important system activities with the possibility of filtering these according to a variety of criteria (user, IP/MAC Address, message) and to download this as a CSV file for further processing.

3.7.2 Statistics

Revenue

Graphically displays the revenue statistics over a certain period of time.

Value	**Description**
from	Start of search scope.
to	End of search scope.
Filter	Filter the selected value.
Search	Searches the entered value.
Reset	Resets the entered search.
Hide Chart	Check to hide the chart.
CSV Export	Exports the data table below as CSV.
XLS Export	Exports the data table below as XLS.
Reset Zoom	Resets the zoom which was used on the chart.

Traffic

Graphically displays the traffic statistics over a certain period of time (upload, download, total traffic).

Value	**Description**
from	Start of search scope.
to	End of search scope.
Search	Searches entries for the entered settings.
Reset	Resets the entered search.
Reset Zoom	Resets the zoom which was used on the chart.

General

Graphically displays the statistics of Ticket Templates used, Modules used and Tickets/Language over a certain period of time.

Value	**Description**
from	Start of search scope.
to	End of search scope.
Search	Searches entries for the entered settings.

Value	**Description**
Reset	Resets the entered search.

Tickets

Shows the ticket statistics as table over a certain period of time.

Value	**Description**
from	Start of search scope.
to	End of search scope.
Filter	Filter the selected value.
Search	Searches entries for the entered settings.
Reset	Resets the entered search.
CSV Export	Exports the data table below as CSV.
XLS Export	Exports the data table below as XLS.

3.7.3 System

Shows the output of the last operating system logs and mail server logs.

3.7.4 Hardware

Shows the system overview and the health status of your hardware.

Value	**Description**
System Overview	E.g. IP Address of the system in the 'Office-LAN', uptime, CPU load.
Hardware	E.g. processor model, CPU speed, PCI devices.
Network Usage	Network card information.
Memory Usage	E.g. free/used memory.
Filesystems	E.g. partitions, free/used.

3.7.5 Connection Tracking

(if activated) You can search through the HTTP proxy server logs (websites visited) and connection logs of all 'Surftickets'.

	Blocked content from Web Filter is displayed in red.
	You have to comply with your national legal regulations when using this feature.

Action	**Description**

Live View	Displays log entries in real-time.
Search download	Provides search result in raw format (50000 lines limited).
Logfile download	Provides logfiles in raw format (unlimited lines).

3.7.6 Messaging

View and download messaging activities from the SMS module, Email module, Social Login module and Data Collector templates.

3.7.7 Active Clients

Displays a list of presently active clients.

4 Customer Logon

	Your guests do not need to make any changes to their devices (e.g. laptop) or to install any software. With 'real Plug and Play', guests automatically see the customer's logon page when they start their web browser.
	Do not close the ticketstatus window which appears after successful logon.
	Use http://logon.now for re-logon or status info.
	Use http://logoff.now to force a logoff.

First of all, your guests need to connect to your so-called 'Surf-LAN' (e.g. network cable, WLAN).

Please contact your system administrator for further information.

When attempting to access a web browser (e.g. Internet Explorer, Firefox, Safari, etc.) for the first time, the logon page automatically appears on the guest's computer. This page is in several languages.

A guest can enter his/her access data and are then activated for unrestricted Internet connection (exception: a security filter has been activated).

The guest now has the following options to establish an Internet connection:

4.1 Ticket Logon

To get an Internet connection a user has to enter Username and Password as shown on the 'Surfticket'.

The system supports Ticket Expansion. This function enables the guest to logon with a new ticket before the duration of an existing ticket expires.

4.2 Room Logon

(optional) If your system supports a 'PMS' connector, a guest can generate his/her own ticket by entering his/her personal details (depends on 'PMS' system). If the values are valid, the guest is routed to an overview, displaying all ticket types available for this module.

After selecting a 'Surfticket' the guest is accordingly activated for the system and the