

1. HSMX 5.0 manual

1.1 Introduction

The HSMX Gateway is a platform designed to manage authentication and billing in your network. It provides a role based intuitive management platform to manage your network and users. Thanks to the included Lawful intercept module, you comply to the regulations in place to store connection history of your visitors.



The system can be split up in a few big parts:

- User management
- Portal page
- Billing packages
- Settings (system / modules)
- Network configuration
- Reporting

Configuration over the web interface. There is a limited shell interface to perform basic troubleshooting and configuration.

1.2 Initial setup

1.2.1 Introduction

The first time configuration can be done in 3 ways:

- Console (Shell access only)
- Connected to the LAN port with DHCP client enabled (Shell or web administration possible)

- Connected to the WAN port with a static ip (Shell and web administration possible)

After the preferred method is chosen, the network configuration can be set and configuration can continue over the web interface.

1.2.2 Console

Connect a keyboard and screen to the back of the HSMX appliance, verify the keyboard layout and login with the default credentials (admin / admin).

The shell allows you to do the basic network configuration in order to get the network connectivity up and running and to continue the configuration over the web interface.

For more information on the feature set of the shell, read section 1.3.

1.2.3 connected to the LAN port with DHCP client enabled

Connect your computer to the LAN port (the LAN port should be identified on the quick configuration guide). You should receive an ip of the gateway in the subnet 192.168.80.0/24. You can now connect to the web administration console via [http\(s\)://192.168.80.1](http(s)://192.168.80.1) or login over SSH to get access to the Shell and log in with admin / admin.

1.2.4 connected to the WAN port (static ip via auto configuration ip)

Connect your computer to the WAN port (the WAN port should be identified on the quick configuration guide). You need to configure your computer with a static ip (10.10.10.2 / 255.255.255.252). You can now connect to the web administration console via [http\(s\)://10.10.10.1](http(s)://10.10.10.1) or login over SSH to get access to the Shell and log in with admin / admin.

1.2.5 next steps

On the web administrative console, go to network => network configuration and configure the network settings for your network, after that you can continue the configuration over the configure ip address.

On the Shell, type configuration , ip and follow the wizard to configure the WAN ip address.

2. Web administration interface

2.1 Introduction

The web administration interface is designed to be intuitive and can be adapted to your needs as well as the needs for any administrator of the system whether it is a front desk administrator that needs to do user administration, the IT department that needs to troubleshoot the system or

accounting personel that needs reporting.

Each administrator can be limited to the modules they are allowed to work on, they can get full administrative right or read-only access.

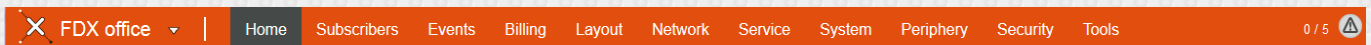
Additionally each administrator has the opportunity to configure its own dashboard with the widgets that matter and in the order or size wanted.

Each administrator can also create its own favorites menu with the modules and pages that matter the most so it is easy to navigate through the system.

2.2 Structure

The administrative console consist of multiple layers, each layer has its own sections:

2.2.1 layer 1 - top menu



2.2.1.1 Site name

Site name is configurable in system => settings, the site names is also the title of the page in the browser so it is easy to identify the correct HSMX when administring multiple HSMX gateways in a tabbed browser.

2.2.1.2 Action Menu

The action menu (the small triangle) opens a sub menu in the second layer. It contains a link to logout from the administrative console and it contains links to all HSMX gateways connected to the system.

2.2.1.3 Main menu

The main menu contains the links to every module on the HSMX, it is logically divided in a number of sections. It has 2 modes of operation, hover or click, this can be configured in System => settings. When you click (or hover) an item, it will open up the submenu related to the section in the second layer. This layer will always stay visible, even if you navigate to different modules within the same section.




2.2.1.4 Counter

Next to the main menu you'll find a counter, this shows you how many authenticated devices there are compared to the amount of connected devices.

2.2.1.5 Health status

The health status (top right) is a quick overview if all services operational and if network problems are detected.

There are 3 states:

-  healthy, all services operational
-  warning, some services not operational, not completely service impacting.
-  critical, service impacting erros detected

By clicking the icon you get a list of all services and checks and their status.

It is also possible to get this list through e-mail when an event happens, configurable in system
+> settings (health report)

2.2.2 layer 2 - Submenu



The submenu also consist 2 sections:


- *modules*


This list of modules depends on the selection in layer 1, the current active module is coloured so you can easily identify your current module.

- *actions*

This is a list with action icons, the actions depend on the currently opened module so it might be an icon to add a new billing package if you're on the billing module or an icon to add a portal page if you're in the portal page section.

2 common actions that can be found on most pages are:

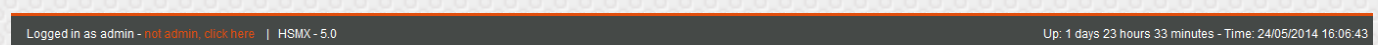
 add this module to your favorites

 view the inline help of this module

2.2.3 layer 3 - body

The body section content depends on the selected module, it can also be the dashboard.

2.2.4 layer 4 - Footer



The informational footer contains the follwoing data:

- admin user logged-in
- HSMX version
- Uptime
- System time

2.3 Navigation

2.3.1 introduction

Navigating through the administrative console is made easy and efficient by creating an intuitive and logical grouping of all modules.

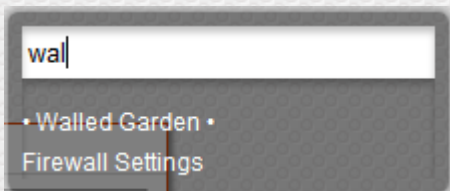
Additionally there are several ways to navigate through the system.

2.3.2 Using the menu

Using the logical structure (explained in 2.4) you can easily navigate through the system, since the submenu is always visible it also very easy to see all related modules allow for easier navigation to the related modules.



2.3.3 Using the search

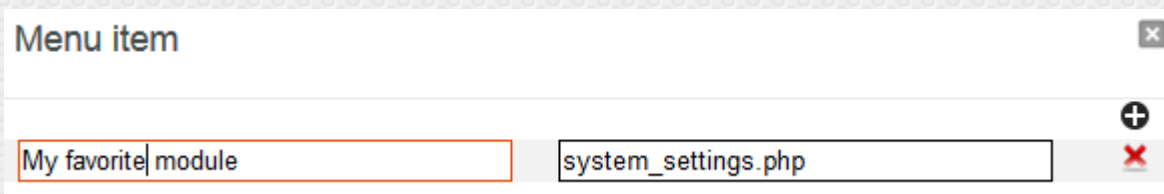
When you click anywhere in the menu, it is possible to start typing the name of the module, you will see a list of modules that correspond to what you typed and you can use the arrow keys to navigate through the list and press enter to navigate to the module.



2.3.4 Using the favorites menu

With the favorites menu, you can make a collection of your most used modules for quick navigation, the favorites menu opens up when clicking home in layer 1.

To mark your modules as favorite, click on the star  that is visible in each module on the second layer. This opens up a list of configured favorites, press  to add the current module to the list and give it a descriptive name. See the picture below as an example.



2.4 Logical menu structure

2.4.1 Home

The home section contains a link to the dashboard and also contains the collection of modules you marked as your favorite.

2.4.2 Subscribers

A list of modules to manipulate the user database as well as to real-time activate and update users.

2.4.3 Events

A list of modules to plan / manage events as well as tools to integrate in the network infrastructure to give the event planner an additional dimension. E.g. create a separate wireless network dedicated to the planned event.

2.4.4 Billing

A list of modules to setup all tiers of service available in the system. The packages / tiers defined are used for billing purposes but also serve as a template with all settings related to the subscriber database (speed / timeout / QoS / ...)

2.4.5 Layout

A list of modules to manipulate the portal page look and feel as well as the templates.

2.4.6 Network

A list of network configuration tools, here you configure all network interfaces (both LAN, WAN or management) and configure services such as DNS, 802.1X, DHCP, ...

2.4.7 Service

A list of all gateway service oriented modules, (redirection, walled garden, authentication modules)

2.4.8 System

All system wide tools, (backup / restore / reboot / performance / ...)

2.4.9 Periphery

All the modules related to external applications / tools / devices and interfaces.

2.4.10 Security

Security related features such as the firewall, intrusion detection and SSL.

2.4.11 Tools

A selection of tools that can be used to troubleshoot or generate reports.

3. Homepage

3.1 Introduction

The Home screen is a strategic overview of the system, this is the place where you can monitor the system in glance. The content of the home screen can be personalized and can consist of the following widgets:

- Locations
- Leases (used IP addresses from a guest network)
- Health
- Filters (rules configured in the redirection daemon module as well as the portal hits)
- Bandwidth report
- Packets (amount of billings bought)
- Subscribers (active, idle and pending subscribers)
- User license
- Update
- Monthly statistics
- User statistics
- Log
- Revenue
- Rooms
- Subscriber networks
- Devices
- Webserver connections

3.2 Usage

To activate the widgets, click on the jigsaw icon in the submenu. On this page you can activate or deactivate the widgets by clicking the checkbox of the corresponding widget. The widgets are then displayed on the front page, you can reorder the widget to the location of your choice. This page is personal so each administrator can update it to its own preferences.

4.0 User management

4.1 Introduction

The HSMX has a very powerful user database, the user database can be populated in many ways.

- Voucher creation via the web interface by an admin or receptionist

- Auto generated accounts with the hospitality module (hotel PMS integration)
- Self-registration by the client on the portal
- Accounts generated by the UMS application (easy to use voucher generation application)
- Accounts generated by ticket printers
- Accounts added via the XML module (by external authentication systems)

The web interface allows you to view / search update and delete these accounts on your system as well as export the user database.

4.2 Activate subscribers

4.2.1 Introduction

This module allows you to authenticate devices that cannot authenticate on their own. This could be a browserless device or a device with too strict browser / security settings that cannot open the portal page.

4.2.2 Use

To activate a subscriber simply select the correct MAC or IP and choose a billing plan. As soon as the billing plan expires or the subscriber goes offline, he or she will need to authenticate or the device needs to be activated again.

If you choose MAC based billing, the subscriber will always be able to go online without authentication, even if he went offline.

You can optionally specify a user name to easily identify the device later on in the overview.

The option login with an existing account, logs the user in with an existing account rather than creating a new one.

4.3 Add device

Mac addresses added here will either be blocked or activated automatically when establishing a connection. You can remove or update these devices by going to subscribers -> overview -> mac list.

Note that mac based authentication only works when this feature is enabled in the performance menu. (system -> performance)

4.4 Create subscriber

4.4.1 Introduction

This module is designed to add subscriber(s) to the system. This can be done one by one (add subscriber), by batch (create vouchers) or by uploading a CSV file (upload).

Depending on system configuration (see general settings - voucher code only) you have a username / password field or only a voucher code.

4.4.2 Create

Fill in the desired fields, pick a billing and template and press create. The system will store the user and create the voucher specified. Vouchers can be viewed at any time in subscribers -> voucher list.

4.4.2 Upload

When uploading a file make sure the columns match exactly what is configured in the customize csv section.

4.4.3. Advanced settings

If more options are needed you can open the pane of advanced settings.

- Client information (address / contact details / company, ...)
- Expiry timeout, start date and end date will overwrite the configuration of the chosen billing plan. So only fill these in if you want to use a different date or timeout.
- Send charge to room(Hospitality module): Use this option if you want to send the charge of the created account to the guest room folio. This will open a popup where you can search for the guest.

4.5 Subscriber overview

4.5.1 Introduction

This module shows all users in the user database and connected devices. The listed users can be updated / deleted or logged out when they are online. It is possible to change the order and available fields of the list by clicking on the icon right of the column names. Move items from the right side to the left to include them in the view. If the left side is already filled up, you need to

move the items you don't want to see from the left to the right.

Some fields have an info popup, they have an icon (ℹ️), when you click on it a popup will open with more information. When you click next to the username, you see the current package details and the original billing plan details (for comparison). You can also click on the bandwidth to see the current throughput of this subscriber.

4.5.2 Sections

- Active: Subscribers/Vouchers that are currently logged in.
- Pending: Devices that are connected to the network but are not authenticated yet.
- Idle: Subscribers/Vouchers that have logged on and logged off again.
- Expired: Subscribers/Vouchers that have been used up.
- Unused: Subscribers/Vouchers that have not been used yet.
- Archive: Expired subscriber/Vouchers moved to a separate archive table (Usernames in this list can be reused.)
- Blocked: Subscriber/Vouchers that have been blocked.
- Mac list: A list of all MAC addresses that no longer needs authentication when mac based authentication is enabled.
- Connected devices: a real-time view of all devices which established a connection to the internet

4.6 reload cards

4.6.1 Introduction

Reload cards can be used to top up existing accounts. Enter the number of reload cards that need to be created, as well as the prefix for the reload code (this is to keep the codes similar). Select the billing plan and template, and click "Create".

In the advanced settings box, there are some additional options available.

- Type
Export to a CSV file instead of a template.

- Voucher code

Specify the format of the generated vouchers:

- o Numeric
- o Alphanumeric
- o Numeric / alphanumeric

- Number of characters

Number of characters allows you to specify the length of the generated reload cards.

4.6.2 Other tabs

The other tabs list the existing reload cards.

- used: Reload cards that are used to top up other accounts
- unused: reload cards created but still unused
- search: Search for a specific reload card
- list: A list of the generated templates with reload cards that can be used for re-printing.

4.7 Subscriber Search

4.7.1 Introduction

In this module you can search for a specific subscriber that matches your search criteria.

4.7.2 Search criteria

- username
- city
- country
- e-mail
- fax
- first name
- last name
- phone
- state
- street + no
- ZIP
- Company
- room (in combination with the hospitality module)
- MAC

- Any custom field configured in Service -> custom fields

These search criteria can be combined and regular expressions can be used to make the search very powerful.

There is a regular expression helper next to the search field, when the regular expressions works on the example it will be marked yellow.

Results

After search the results are displayed, you can click on the information icon next to the subscriber to update or view the details.

By clicking the checkbox in front you can delete or batch delete the subscribers returned by the search engine.

4.8 Settings

4.8.1 Subscriber table

These settings will clean subscribers from the subscribers table (subscribers -> overview)

4.8.2 Subscriber creation

When unique serial number per batch is enabled the system will keep increasing the serial number per voucher. If not enabled the system will start over whenever a new batch of vouchers is created.

4.8.3 Device connectivity

Period of no activity in minutes after which connections will be removed and accounts become idle. Configuration is applied after restarting the guest networks.

A list of all connections can be seen in subscribers -> overview -> connected devices.

4.8.4 Bandwidth utilization

This feature stores bandwidth usage per subscriber which can then be viewed in a graph. Enabling this feature when handling many authenticated devices may carry a performance penalty.

4.9 Voucher list

This lists the templates of all the vouchers that were generated on the system. From here you can download them for re-printing or delete them from the system.

5.0 Events

5.1 Introduction

Adding an event is similar to adding an account but with support for additional features. People will be able to login with the username created here and the event name will be shown in the calendar overview.

Additionally you can choose to execute functions based on the start and end date of the event.

5.2 Calendar

An overview of all created events, clicking on a date will open the dayview window where you can see the start and end date of an event and the possibility to alter the account.

5.3 Functions

Functions are shell commands that can be executed on an external device. To add functions:

- Add the device where the commands will be executed (devices tab)
- Create a batch and attach it to a device (functions tabs)
- Add the commands (click on the gear icon after adding a batch in the functions tab)

When adding commands you can make use of dynamic variables by adding a word between { }, these variables will then be asked when creating an event and replaced when executing. For example: add ssid {ssid}, when we now create an event and enable this function, the system will ask us the value to replace {ssid}. At time of execution the word between { } will be replaced by the value we entered when creating the event. This way you can reuse the same batch for different purposes.

6. Billing

6.1 Introduction

The billing menu is one of the major configuration items of the gateway. Here you configure all the different billing packages available to your subscribers.

There are three types of billings plans:

- Pre-paid billings plans: Guest pays in advance for a pre-defined time or volume

- Post-paid billings plans: Guest pays after use of his connections, price depends on time and/or volume (only in combination with our PMS module)
- Free-access billings plans: Guest does not pay for the access for a specific time period or a specific amount of data volume, the free-access plan supports the recurrence value, this will determine how many times a guest can choose a free billing plan

6.2 Billing overview

The overview page displays all the billing packages, it is possible to group billing plans to keep them organised. When billing plans are deleted but still tied to a subscriber profile, then they are not really deleted but hidden. Staff billing plans are only visible for admin users who have the staff option checked.

6.2.1 Adding a billing plan

Adding a billing plan can be done via the add icon in the navigation bar, you will have to select between pre-paid / post-paid or free access.

6.2.2 Options

- Name: Name of the package the subscriber subscribed to.
- Description: Description of the pack
- Price: Value of the package
- Bandwidth up (kbps): The maximum available upload bandwidth available for this profile in kilo bits per seconds.
- Bandwidth down (kbps): The maximum available download bandwidth available for this profile in kilo bits per seconds.
- Small bandwidth up/down (kbps): A fall back bandwidth available to the guest when the subscriber used up all available data volume (only when configured).
- Small bandwidth reset: After this period, the full bandwidth is available again.
- WAN connection :All clients with this billing will use the selected WAN connection (only available when load balancing is enabled).
- URL Redirection: This is the URL that the user will be redirected to after login
- Staff :This option makes sure this package is only available for staff users. Staff users can be

created in system -> access control

- Volume up: Available upload data volume, after that the package will expire or fall back on the small bandwidth configured.
- Volume down: Available download data volume, after that the package will expire or fall back on the small bandwidth configured.
- Network policy: A network policy (client firewall) tied to this package (see Network policies)
- QoS Profile: A QoS (Quality of Service) profile tied to this package (See QoS)
- Content filter: The content filter tied to this profile (optional module) (See Content Filter)
- Upsell: When this is enabled and the system has available public ip's, the client will be natted to a unique public IP (one2one NAT)
- Idle-Timeout: The client connection will be closed after inactivity, the timeout can be configured here.
- Session timeout: How long the account can be logged in. When the connection is closed, this timer also stops so they can reuse the remaining time at a later date.
- Expiry timeout: How long the account is valid after first login.
- Expiration after creation: How long the account is valid after creation
- Start date: The account is only valid after this start date
- End Date: the account will expire at this date.
- Time based access: the account can only log in between start and end hour.
- Calendar days: The account is only valid on the days /hours specified in this calendar day configuration.
- Location: The account is only valid in this location.
- Simultaneous use: How many simultaneous clients can connect with this account.
- Limit account to x MAC addresses: The total amount of devices that can connect to this device, this is for the entire lifetime of the package so not just simultaneously.
- Max concurrent packages: When too many valid accounts with this package exist, it will not be offered to new subscribers in order to ensure proper service.
- Recurrence (free billing packages only): indicates if, how and when this free package can be resubscribed to when it expired.
- Expire: When the account will expire, usually initialized after first login.
- Delay expiration, if the package has the option set to expire on guest checkout (Hospitality module) an timeout can be set so the account is still valid for a few hours after checkout.
- Sales outlet: (Hospitality module), A sales outlet can be used when charging this account.
- Group: (See group settings) A profile can be tied to a subscriber group. With these groups, it is possible to allow or deny access for the entire group, interesting feature for educational use.

6.3 Upgrade Packages

6.3.1 Introduction

A new way to give an upgrade path to users is by using upgrade packages.

Upgrade packages allow a client to update their current package rather than buy a complete new package.

Upgrade packages are tied to a billing plan, this makes it possible to differentiate the upgrade

packages depending on what the customer already has. E.g. when a user is already in a high bandwidth package, you can only show packages to update time / amount of connections. When they are on a low bandwidth package you can show upgrade to upgrade bandwidth.

Upgrade packages are an ideal way to up-sell standard free Internet access and generate revenue.

6.3.2 Configuration

In Billing -> settings you need to configure the system to use upgrade packages instead of the standard billing plans. Check the option upgrade packages.

Since the upgrade packages are tied to a billing plan this is also the place where you need to add the upgrade packages. Go to billing => billing plan and click on the upgrade icon right of the billing plan where you want to add / edit an upgrade package.

In the upgrade package you can configure what needs to be upgraded (more time / volume / bandwidth / connections, ...).

The option "Calculate price based on remaining time" will deduct the price you configure depending on how far your initial package has progressed. E.g. if you used up 50% of your package, you will only pay 50% of the upgrade price.

The option "Upgrade package to" will set the billing plan of the client to the billing plan you selected so after the upgrade, the client will get the upgrade options of the new billing plan.

As soon as you created the upgrade packages they will be automatically become available for your clients as long as you have an upgrade compatible portal or use a portal from the portal page editor. (Make sure upgrade packages are enabled in general settings.)

6.4 Calendar days

Calendar days allow you to specify special recurrent days and moments. It can for example be used to specify all holidays.

These calendar days can be tied to a billing plan, accounts create with this billing plan are only valid on the dates time configured in this calendar day.

6.5 MAC based

Here you can configure some limitations that are set for mac based users, these users have no authentication but with this module you can still give them some limitations.

6.6 Settings

6.6.1 Session time

Define how the session time will be calculated when the guest logs off. You can choose between the time he started and stopped his session or the actual period activity was detected.

6.6.2 Billing

Configure the VAT rate and currency to be used in reports, invoices, ...

6.6.3 Upgrade settings

When a guest browses to the upgrade domain you can choose to either upgrade his current plan or let him buy a new full plan. When you want to show upgrade packages you have to enable the "upgrade packages" checkbox and create packages in the billing submenu.

When full plans are shown you can additionally choose to ask full price or rebate a part based on the remaining time of the current plan.

Note: when using a custom portal your portal needs to contain the logic to support the above, please contact support for more information.

7. Layout

7.1 Introduction

Here you can adjust the appearance of all the different aspects of your HSMX Gateway.

- Portal page : The page that the subscriber will see when logging onto the Internet.
- Logout Console: Box that will popup when the user has logged on.
- Templates: The templates that will be used when printing out Vouchers or invoices.
- Logout page: Page shown when a guest logs out.
- Registration forms: configuration on how a client should register.

7.2 Logout console

A logout console is a small popup that guests will see when they login. A logout console can show the remaining time and volume and has a logout button. The logout console needs to be enabled in the (portal page) rules..

There are 2 types of logout consoles:

- HSM logout console, this is a build in logout console where you can easily change the colors and text.
- Custom logout console, this is a fully customizable console, to change the layout you need to download the console first (HTML knowledge is required).

7.3 Logout page

The logout page is a page where the client will be redirected to after they logout. Upload a ZIP archive that contains "index.html"

7.4 Portal page

7.4.1 Overview

Here is a list of all portal pages, they can be edited or deleted. In the navigation bar there is an icon to add a new portal page.

Note The (portal page) rules determine what portal will be displayed to the client (See Rules).

Depending on the type of portal, the portal can be uploaded or a SFTP account can be setup to transfer the portal to the gateway.

7.4.2 types

There are 5 types of portal pages:

- HSMX portal: this is the standard and built in portal, you can change the entire look and feel with the portal editor.
- External: a portal page that is hosted on an external web server.
- Custom HSM portal: this is also a standard portal but can be fully customized, to change the

layout (colors,text,...) you need to download the portal first (you can do this when editing the portal) and alter the pages manually (HTML knowledge is required).

- Hospitality portal: a portal page like the custom HSM portal but with advanced PMS functionalities (view bill, text messages, check out).

- HSM portal: (deprecated) you can only change the colors and text.

7.4.3 portal options

Login settings

- Voucher code, this is a standard username/password login. You can also make this voucher code only in settings -> general settings

- In house guest, with this option guests can login with their room details (configured in settings -> PMS settings). Make sure PMS is enabled as payment method in the portal rule or the room fields will not be showed.

If PMS is enabled in the portal rule but in house guest is disabled, the gateway will show a "new user" button on the portal page which customers can use to create a voucher by entering their room details (charge will be sent to the PMS system).

- Registration forms, gives the ability to register before being able to authenticate.

Allow billing plan change on login

With this option enabled, guests will always be redirect to the plan page even if they have a valid account.

7.5 Registration forms

Registration forms can be used to create accounts on the portal and capture data while doing so.

! The registration form needs to be enabled while editing the portal page and the portal page needs to have the registration logic (portals created by the portal editor are already compatible with the latest features).

Form fields

These fields will be showed on the portal page and stored in the database for future use.

Placeholder and HTML5 validation are both HTML5 depended and will thus not work if the browser displaying the portal has no support for it.

The validate option has 3 options:

- No validation: the field is optional
- Not empty: the system will not check the input, the only requirement is "not empty"
- Advanced: this option is based on regular expressions, the system will check if the input matches the expression entered here

Username & password creation / Authentication

How the system will generate the username and password if registration is successful.

- No username: the system will generate an username with the details of the device (IP or MAC), auto login is required for this option.
- Use guest data: one of the "form fields" can be used as username, the password will be generated by the system
- Generate username: both username and password will be generated by the system
- Manual: the client will be able to fill in his username and password during registration

! Username will be ignored when voucher code only is enabled.

As additional option you can enable oAuth. This is a framework being used to support third party login details (Facebook, Twitter, ..., any company using oAuth). With this option enabled the system will redirect you to another portal (for instance Facebook login) to complete registration. The system is also capable of fetching user info from this third party (like e-mail, if the software allows it).

OAuth

The system has some predefined values where only the client secret and client Id is missing. These values (together with the fields that can be captured, see data capturing tab) can be found when creating an APP on the third party server (Facebook, Twitter, ...). To add more predefined values you can always contact us at support.fdxtened.com, this way we can see if implementation is possible and if we can add it to the predefined list.

More information regarding a manual API configuration can be found here:
http://download.fdxtened.com/oauth_manual.html

The walled garden tab can be used to open a specific IP / domain to allow redirection without being validated, this is needed when redirecting the customer to, for instance, Facebook.

On success

This section will determine what happens when registration is complete, options are:

- Show message: this will show a message on the portal (the php variable \$error needs to exist on the portal)
- Redirect to internal page: this page needs to exist in the portal (login.php for example)
- Send e-mail: the system will send an e-mail to the customer, the SMTP settings configured in system -> system settings will be used.
- Send SMS: an SMS will be sent to the customer, this can be via SMTP or via an HTTP request. For more information see the SMS gateway which will be used.
- Autologin: the system will login the subscriber without showing the portal again.

! Settings can change during configuration depending on how the system should behave. For example the form field e-mail will be required when enabling the option "send e-mail".

Misc

Name: name of the registration form

Visible for portal use: make the registration form visible for portals

Visible for admin interface: adds the registration form to the "add subscriber" menu (registration form will be ignored if authentication method is set to "no username")

7.6 Registration forms

7.6.1 Portal session

Session cookie

A new feature that allows clients to connect even if they are blocking cookies, since the session is passed on page by page via the sessionid.

The portal needs to be compatible with this feature, the portals built with the portal editor are automatically compatible with this feature.

Message for portal session error. This error is returned when Use cookies is enabled but the client block cookies.

Portal session error

When cookies are enabled, the portal session error shows up when multiple portal sessions are done with the same sessionid (e.g. multiple tabs in browser).
When this is detected we will show this message.

7.6.2 Templates

Templates that will be selected in the admin interface, you can change the template at any time when creating accounts.

7.6.3 Voucher code only

With this enabled the system will set the password equal to the username.

7.6.4 Password policy

Configure the password policy being used on the portal page, password policies can be used to make password changes mandatory.

7.7 Templates

Here you can upload or create your own template, these templates are used for printing vouchers, invoices, etc. To upload a template you can click the icon in the upper-right corner, these templates have to be in RTF format. To create a template with the build in text editor you can press the create icon .

Templates created with the build in text editor can be used to generate a PDF file or as popup when creating vouchers, where uploaded templates will give you an RTF file.

Available variables

Vouchers

```
||user||  
||pass||  
||country||  
||state||  
||zip||  
||street||  
||city||  
||email||  
||phone||  
||fax||
```

Reload card

||date||

Vouchers and reload card

||description||

||session_timeout||

||volume_up||

||volume_down||

||expiration||

||expire_time||

||band_up||

||band_down||

||url_redirect||

||sim_use|| -> simultaneous use

||idle_timeout||

||limit_mac||

||price||

||sn|| -> voucher serial number

||creator||

||bill|| -> billing plan name

Invoice

||voucher_code||

||description||

||number|| -> invoice ID

||price1|| -> price

||price2|| -> price

||company||

||lastname||

||firstname||

||address||

||city||

||country||

8. Network

8.1 Introduction

Here you will find the most important network related settings including the guest network.

- Network configuration (WAN & LAN)
- Firewall
- Cluster
- Network policies

-...

8.2 802.1x

8.2.1 Introduction

802.1x provides an authentication mechanism for clients connecting to the WLAN. When a client enters his access credentials the wireless controller will consult the gateway, if valid the client will be allowed on the network and activated on the gateway at the same time.

8.2.2 Configuration

- Add the IP of the wireless controller as well as the radius secret in the access point list
- Upload a valid SSL certificate
- Configure the access point to use the gateway as radius server (the same radius secret needs to be used)
- Open port 1812 protocol UDP in the firewall

8.3 Cluster

Introduction

The cluster module creates a high available redundant system from 2 standalone HSMX gateways.

Operation

During normal operation the 2 nodes in the cluster are available but only one of them operates the LAN networks and has the configured virtual IP.

The 2 nodes communicate with each other and verify the cluster status at all times. When the active node becomes unreachable or when a problem is detected (e.g. disconnected LAN cable) a smooth fail-over process will be initiated so the slave node starts operating the LAN network. The other node will immediately join the cluster again as slave node.

Configuration

Network configuration

The cluster communicates over one of the configured interfaces of the system. This can be the standard WAN interface or a dedicated interface used only for the cluster. The interfaces can be

configured in Network => Network Configuration.

Firewall configuration

In order to allow the devices to communicate and synchronize with each other some firewall rules need to be added.

!For safety reasons it is best to include the source IP of the other node in the rules so the services cannot be exploited by other systems.

Open the following ports for the source IP of the other node in Network => firewall settings.

- TCP port 80
- TCP port 873
- TCP port 5432
- UDP port 5555

Cluster advanced settings

- Ping pongs: *Number of pings before the system performs a health check of the other gateway.*
- Max failed pings: *Number of failed pings before the slave becomes primary.*
- Max failed healths: *Number of failed health checks before the slave becomes primary.*
- Ping interval: *The interval in which the ping commands are sent.*
- Sleep after health check: *How long the scripts sleep after a health check.*
- Ping timeout: *The timeout before a ping command is marked as failed.*
- Health timeout: *The timeout before a health message command is marked as failed.*

note *All time based values can be written as seconds or seconds,microseconds (comma separated) like: 5,5000. Microseconds are optional.*

Cluster settings

The cluster settings are divided in 2 columns, one for the settings of the current gateway, another for the settings of the other gateway.

Virtual IP

Here you can configure virtual IP's, the virtual IP will always point to the active node so usually a virtual IP should be chosen on the network used to configure the gateway cluster. Specify the IP / sub-net and network port where this needs to be applied to. Optionally a second virtual IP can also be chosen.

Communication IP's

Here you can configure how the 2 gateways can communicate with each other. Usually a dedicated network port is used to sync all data between the 2 gateways; a backup interface can also be configured to avoid a single network failure causes communication loss between the 2 gateways. Configure the network interfaces first in network => network settings.

Cluster status

Here you can verify if the 2 gateways can communicate properly with the configured IP addresses and if the firewall is properly configured.

Click on the button test connection to check the communication works, if a red cross appears communication is not working; verify if the network configuration is properly done and if the firewall is properly configured. Only after the connection is green it is possible to enable the cluster.

Network interfaces

The entire network configuration is shared between the 2 gateways in the cluster. This is because they share the IP aliases / PPPoE connections. They are activated on the primary node only. This means there is one more step; you have to configure the IP's of the other gateway for interfaces that are already configured. There is a small icon that will try to get the information from the other gateway, this works if the interface names are identical.

8.4 Connection tracking

All clients that are using a protocol configured in connection tracking will be destination natted to one of the available IP's (to add an IP go to network settings). This can be used for services that require a unique public ip per accepted connection. (VPN / web apps / ...)

8.5 DHCP

8.5.1 Introduction

Here you can configure the DHCP server, configuration is based on subnets so if no subnets are shown you can either create a guest network in network -> network configuration or add a subnet in network -> subnets.

8.5.2 Configuration

DHCP server

LAN IP: this is the IP the DHCP server will forward as default gateway, in most cases this will be the IP you assigned to the guest network (network -> network configuration).

Start - end IP: this is the pool the server will use to assign IPs, you can view the available/used leases in the graphical reports.

Lease time: will determine how long a lease (given IP) will be reserved for a specific client, if the client is no longer connected and the lease expires the IP will be available again.

DHCP rules With rules you can assign a specific MAC or VLAN to a subnet. You can use a wildcard (*) for MAC addresses. (44:58:66:*:*:*)

When the system will detect a valid rule he will assign an IP from that subnet to the client.

Static DHCP

With static DHCP you can reserve an IP for a specific device (MAC format: 00:00:00:00:00:00).

DHCP options

Options can be used to add additional information to the DHCP request, in order for this to work the client needs to support the configured option.

8.6 DNS

8.6.1 Servers

You can configure up to 3 servers to resolve domains.

8.6.2 Offline mode

When the system is no longer able to resolve domains you can let the gateway resolve all domains to one specific IP (resolve IP), this way the client will no longer receive a timeout error from his browser but will be redirected to the gateway. From there on you can either show a predefined message (not able to resolve domains) or show a portal page (make sure a portal rule is configured with portal rule type offline mode).

The resolve attempts value is the amount of failed DNS records before switching to offline mode, a value higher than 1 is recommended.

8.6.3 Misc

You can block non standard DNS records, this can be used to block DNS tunneling.

8.6.4 DNS entries

Here you can add custom DNS entries, available types are:

- login domain: domain used to redirect to the portal page
- logout domain: domain used by clients to stop their current session
- upgrade domain: can be used to retrieve an upgrade page where they can buy a new plan (only for PMS users)
- status domain: to retrieve the status page, the page can contain information about their current session

- resolve: domain will be resolved to the configured IP
- block: this domain will not be resolved resulting in a browser error on the client
- forward: forward DNS records for this domain to another DNS server

8.6.5 DYNDNS

This module can be used when you have a valid subscription with DYNDNS or NO-IP. Both of them will make sure you can always reach the device via a certain domain if the WAN IP continuously changes (DHCP).

8.7 Load balancing

Load balancing will automatically spread the load of all subscriber sessions over the different WAN interfaces configured here. By default only one WAN interface is added, press on the + sign to add another WAN interface. Make sure you already configured the WAN interface in network settings. The weight determines how much users the WAN connection will get compared to the other. The higher the weight the more users will be assigned to that WAN interface. The option failover allows that an interface can be used when another WAN interface is down.

You can configure a load balancing interface in a billing or guest network to "reserve" this interface for all clients having this billing or connecting through that guest network.

8.8 Network configuration

8.8.1 network configuration

WAN

Static

In this mode, you need to enter an IP address, subnet, network port and optionally the default gateway.

DHCP

Here you only need to choose the network port.

PPPoE

You can choose this option if you want to connect to a DSL device. Just enter a username, password and network port.

You can see additional information (connectivity monitor, advanced port settings,...) by clicking the gear icon.

Use entire subnet can be used to add aliases, all IPs within this subnet will be added to the selected port.

Guest networks

Managed

These networks will handle client traffic between LAN and WAN, clients need to authenticate before they can access the WAN.

Unmanaged

Traffic will be forwarded without inspection or limitations (no configuration to clients can be applied).

Additional configuration such as Layer3, listen to all VLANs, logout IP, ... can be seen when pressing the gear icon

8.8.2 network ports

On this page you can configure the physical Ethernet ports and also create virtual interfaces.

You can create:

- *VLAN interfaces*: enter the port number and the VLAN id.
- *Bridges*: create a bridge interface that bridged 2 or more (virtual) interfaces.

8.8.3 routes

This module displays the current default routing table, it is also possible to see the other routing tables by selecting a different one from the dropdown. This is only used in case of WAN loadbalancing.

On top of the page it is possible to add custom routes, custom routes can be added for WAN and management networks.

8.8.4 Interface order

In case you want to change the default interface order or you bought a Ethernet port upgrade it could be needed to fix or change the interface order. This nice tool helps you with this process, you can see when a link is detected on a network port and you can use that to change the interface order. After a reboot the order will be saved.

Important Keep the first port where it is as it is part of the gateway's license process.

8.8.5 Overview

Check the configuration applied on the system.

8.9 One 2 One NAT pool

Here you can enable the IP addresses that will be used when a client uses a billing plan with Upsell enabled. To add a new IP address or subnet go to network configuration and create an alias on the WAN port.

8.10 port forwarding

8.10.1 Introduction

Port forwarding gives you the ability to connect to a specific device within the LAN network.

8.10.2 Requirements

The device needs to be active and authenticated in order for the port forwarding to work.

8.10.3 Configuration

You need to choose the WAN interface, public IP and port (You will connect to this IP and port from the outside) followed by the private IP and port (this is the actual device in the network that you want to reach).

You can choose a source IP or range if you want to make sure that only devices with this source IP or within the source IP range can use this port forward.

8.11 QoS

8.11.1 Introduction

QoS or Quality of Service makes it possible to provide different priority (bandwidth) to different applications, rules and subscribers. With this functionality you can easily control the bandwidth of all subscribers in your network.

QoS comes standard with every HSMX but with some limitations, to have full access you have to buy the QoS module.

Limitations in the standard version are:

- Tree has only 1 level
- No priorities = no bandwidth allocation
- Only groups are available, network policies (including Layer 7), user profiles and group profiles are not available.

8.11.2 Interface

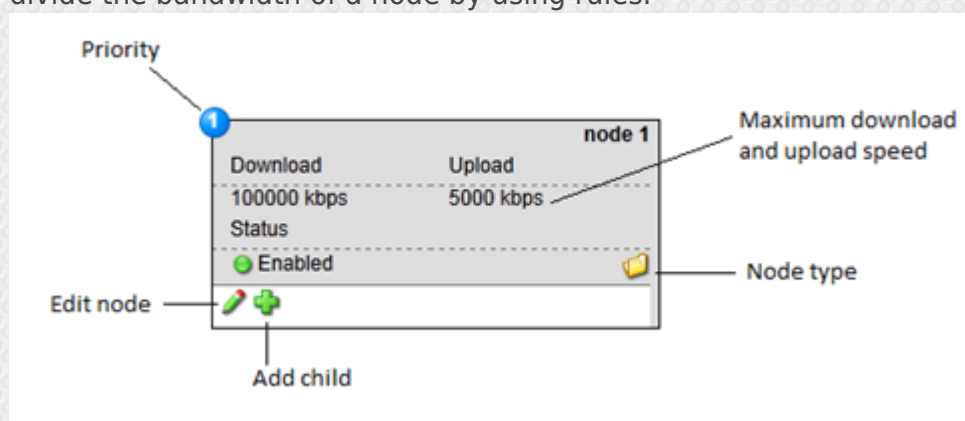
The QoS module is being displayed in a tree view, a rectangle is called a node, all nodes below 1

node are children. The node above one is called a parent node. All nodes are being displayed with their maximum bandwidth (download and upload) and its priority, these go from 1 (highest) to 7 (lowest) and from top to bottom.

Priorities are being used for bandwidth allocation, available bandwidth is first served to users with a higher priority, as soon as bandwidth is available other users with a lower priority will get their normal bandwidth again. The bandwidth of a child can never exceed the bandwidth of his parent.

There are 3 different nodes, this is being displayed by an icon below the status line. To add a child, simply click the green add icon. In the next screen you can then choose which node type you want to add.

If a node shows a funnel icon then this node has a network policy, network policies can be used to divide the bandwidth of a node by using rules.



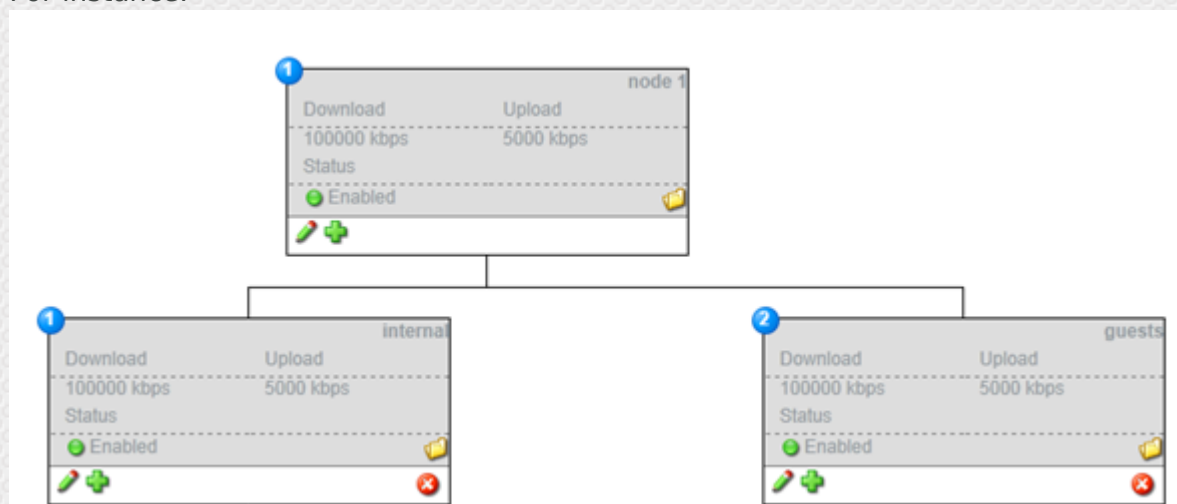
8.11.3 Node types

- Group (folder icon)

This is a group node which is being used to divide a parent node into segments. Group nodes can contain other groups, user profiles or group profiles as children.

Group nodes can be used in a billing plan or location but only if the node has no children. The bandwidth of the selected node will be divided over all subscribers in that node.

For instance:



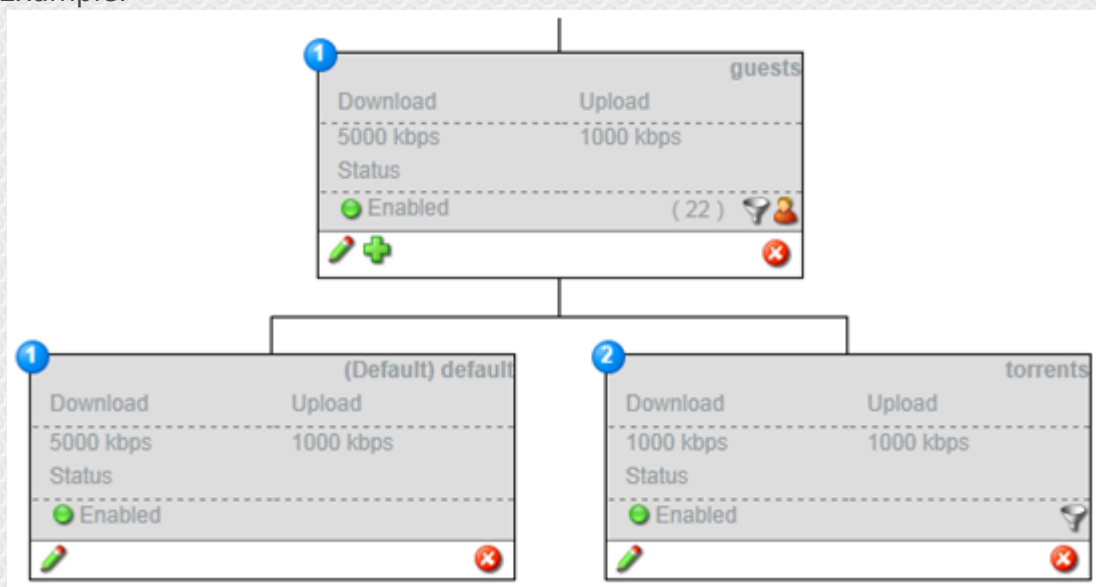
Clients in node Internal will have higher priority as clients in node guests. This means that bandwidth will go from the guests node to internal node if needed. As soon as the internal node doesn't need the bandwidth anymore, the guest node will have his full capacity back. The total download bandwidth of the internal node is 100000 kbps and will be divided over all subscribers in this node.

- User profile (user icon)

A user profile is assigned per subscriber, so if the node has a download limitation of 5000kbps, each subscriber with this profile will have a maximum download limitation of 5000kbps (as long as the total bandwidth of his parent is not reached!).

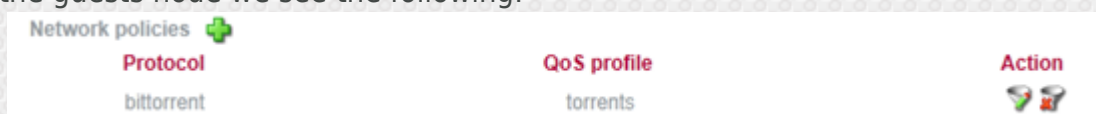
User profiles can contain other nodes (children) to control their traffic, this can be done by creating child nodes, assign them some bandwidth. And finally create a network policy on the user profile node that links to the child node. Traffic that triggers a certain rule will then be handled by that specific node.

Example:



In this example we see a user profile named “guests” and this user profile is divided in 2 nodes, default and torrents. De default traffic has a higher priority and will get all the bandwidth he needs if needed. Node “torrents” has only 1000kbps and cannot borrow from node “default” as he has a lower priority, this means if node defaults needs 4500kbps, node torrents will only get 500kbps.

A funnel is being displayed in the guests and torrents node. This is because the user profile contains network policies and 1 network policy is linked to the torrents node. If we press edit on the guests node we see the following:



This is where we link the application bittorrent to the torrents node. So all traffic from bittorrent will be handled by the torrents node, where all other traffic will be handled by the default node.

Other network policies can be made by pressing the green add icon. Network policies can be made by application, protocol (and port) or after sending/receiving X bytes (Herewith you can

identify large downloads / uploads and give this specific download a lower priority)

- Group profile (multiple users)

This is almost the same as a user profile, but here you define also the total bandwidth for all users in this group. This is designed for simultaneous user accounts.

For instance, you can define a total bandwidth of 5000kbps and an individual of 1000kbps, this means that users will get 1000kbps maximum but the total of all users in this profile will never go over 5000kbps. So as soon as this profile reaches 6 users, users will no longer have 1000kbps (5000kbps/6 users).

8.11.1 Applying QoS

Once the network has been divided into smaller segments (Nodes) you need to tie the QoS profiles to subscribers. This can be done by configuring a QoS profile in a billing plan or a location . If in some situations a client has a QoS profile from a billing plan and one from a location, the QoS profile from the location will be ignored and the QoS profile configured in the billing plan will be used.

8.12 Subnet

8.12.1 Introduction

Subnets are needed when configuring the DHCP server. Subnet entries will automatically be created when a guest network is added so this module requires almost no configuration unless you want to loadbalance between guest networks. A subnet can manually be added by:

- Subnet: configure the IP and subnet

- Hosts: configure the amount of subnets needed (mostly the same amount as guest networks), hosts (available IPs) per subnet and if the system should loadbalance between guest networks. You can press "preview" to preview the subnets before adding them.

8.12.2 Loadbalance guest networks

Since version 5.0 it is possible to let multiple LAN ports (on one or multiple HSMX gateways) operate the same network. This allows for active / active loadbalancing and to support more users and throughput in a high density environment.

Each LAN port has its own subnet but is part of a big subnet, clients will receive an ip from the big subnet by the HSMX DHCP server and the DHCP server will assign different default gateways to the clients in order to loadbalance the clients across all LAN ports.

To configure this you have to add subnets based by hosts and enable the auto distribution option. Once added you can choose the port from the dropdown per subnet.

9. Service

9.1 Introduction

A list of all gateway service oriented modules like:

- Content filter
- Guest authentication
- Redirection daemon
- Walled garden
- ...

9.2 Content filter

9.2.1 Introduction

A content filter can be used to block certain URL's or web pages containing specific phrases. A content filter can be linked to a subscriber network (global settings) or billing package. The content filter comes with a predefined list, this list will automatically be updated if you have a content filter subscription.

9.2.2 Configuration

You can use a predefined list or add a specific value you want to block. You can see the values of a predefined list by clicking on the name.

Available lists:

Banned extensions

If a web page ends with an extension in this list, the page will be blocked

Banned IP's

IP addresses of clients to disallow access to the web.

Banned phrases

Block pages containing words from this list. If you want to block a page containing the word "test" you need to add "test". If you want to block pages containing words that contain "test", you need to add "*test*". This will also block "testing".

Important You can also enable weight. All words on a page that are in your phrase list and have a weight will be added and if the weight is larger than the allowed weight, the site will be blocked. For example, if you have 2 words (test, weight:30 and gateway, weight:31) and the total allowed weight is 50. If you then go to a website that contains the word test and gateway, this site will be blocked because 30 + 31 is larger than 50. If you go to a website with just the word test, this

page will be showed. (if you have 2 times the word test on a page, this will be added as well, so the weight will be 60 for that page)

Banned sites

You can use this list to block an entire site, there is no need for www or http://

Banned URL's

To block a part of a site you can use this list, for example: gateway.com/download.

Allowed sites

This will allow sites that are configured in the banned sites list

Allowed URL's

Allow URL's that are blocked by the banned URL list.

Note A future content filter update can contain a website that you don't want to block, so that is why you can easily make sure that a website is never being blocked by using the allowed lists.

9.3 Custom fields

Custom fields give you the ability to create your own fields that are not by default on the system, like "Date of birth". These fields can then be used in several menus like registration forms, export subscribers,

9.4 Devices

9.4.1 Introduction

Devices are a logical identification of different devices in the system. This has as advantage that you can use the logical device name everywhere else in the system rather than use a technical representation of the device like the user agent or mac address.

9.4.2 Configuration

A device can be identified by

- MAC address: Usually the first digits of the MAC address represent the vendor, this can be used to identify the type of device that is connected.
- User agent: The user agent is a browser identification string that allows us to identify the device, usually the name of the device or the initials are part of the user agent string. With regular expressions you can match a part of the user agent string.

It is also possible to make a device group, a device group can contain several devices. E.g. Mobile devices contain all different kinds of mobile phones.

9.4.3 Use

Devices can be used to

- Show different portal pages based on devices (See portal rules)
- Reporting

9.5 Groups

9.5.1 Introduction

Groups logically group a set of subscriber profiles with the goal to allow or block access for these subscribers. This could be a school that has a group per class, with this option it is possible to block Internet access for the entire classroom.

9.5.2 Use

Group Internet access can be disabled or enabled by clicking the "turn on/off online access" button in the action column.

To add a user to the group edit the user profile and select the group from the drop down (see subscriber details)

9.6 Guest authentication

9.6.1 Introduction

This module will determine how a client will be authenticated, all clients will receive an invalid login message when no authentication mechanism is specified or found.

9.6.2 Use

The system will try all authentication types from top to bottom, once the username is found in one of the authentication methods the system will no longer check other types.

All methods are checked where username pattern is empty or where the pattern is found inside the username. The pattern itself can be regex. The system will strip the pattern, if enabled, before trying to authenticate.

9.7 Location scheduling

Here you can schedule the AAA state of a location. This allows you to open a location (a part of your network) for a configured time period.

Note: Once the start date is reached you cannot update the location scheduling anymore. When deleting a location scheduling or when the end date is reached, the location will return to its previous AAA state.

9.8 Locations

Locations are logical divisions which can be used to apply configuration for a specific part of the network. These logical divisions can be created by adding a guest network (or part) to a location.

9.9 Password policy

In the password policy you can set different password policies for the system. Password policies are used to define actions the user has to do concerning his password. This module can be used for guests and administrators

- Change password on first login.
- Allow the guest to change password on the portal.
- Minimum password length.
- Password expiration.
- Block account after x login attempts.
- Password history (no password that the guest recently used can be reused).
- Password complexity.

9.10 Redirection daemon

Portal filters

Filters are designed to answer to specific User agents, hosts, paths and destination IPs for non active devices. These can be used to perform redirections, mimic internet checks, block unwanted browsers, ...

A few predefined filters can be found in the dropdown menu.

Note: Filters (header + content) are currently limited to 2000 characters

Access log

A list of user agents that reached the portal page.

Proxy

Here you can define some common proxy ports, if someone uses one of these ports a message, configured in return content, will be showed. This way you can tell the customer to disable the

proxy settings before connecting to the internet.

9.11 Rooms

This lists all rooms configured on the system.

This table is populated by:

- PMS: When the PMS module is enabled, the table will show all rooms we receive from the PMS system.
- Manually: You can add rooms manually by clicking the add icon.

Each room can be linked to a floor, guest type and VLAN (you first need to select the subscriber network in order to link it to a VLAN).

Floors can be created in the floors tab, guest types in the guest types tab.

By clicking the edit icon, you can also see all guest details of the guests checked-in in that room.

To ease the search for a specific room / guest, there is a search module available.

9.12 Rules

9.12.1 introduction

(Portal page) Rules specify what options a client has when connecting to the portal. It specifies what

- portal page is shown when a client connects
- what logout console is shown
- what billing options are available
- what billing packages can be bought

9.12.2 Configuration

By adding more than one rule, it is possible to display different portal pages depending on the device type or location.

The rules are processed from top to bottom, as soon as a rule matches, the rules below will be ignored. This is why it is important that the rules are sorted properly, the rules can be sorted by clicking the sort icon in the navigation bar.

The actual rule configuration consist of 2 parts, one is the functionality that needs to be enabled (portal page / billing package / billing options).

The second part is what triggers this specific rule. These triggers can be:

- Default

This is if you want the rule to be run by default

- Location

This is if you want this rule to apply to a location

- All rooms

This is if you want this rule to apply to all rooms (VLAN setup)

- Room

This is if you want this rule to apply to certain rooms, in a range

- Floor

This is if you want this rule to apply to a certain floor

- Guest Type

This is if you want this rule to apply to a certain guest type

- MAC Address

This is if you want this rule to apply to a certain MAC Address

- User Agent Pre-defined

This is if you want this rule to apply to a user agent, e.g. Sony PSP

- User Agent User definable

This is if you want this rule to apply to a user definable agent

- Device

This is if you want this rule to apply to a device type (see devices)

- Subscriber IP Range

This is if you want this rule to apply to a certain IP range

- FIAS rules

Here you can set this rule based on a certain FIAS input, e.g. First name

Note Multiple triggers can be configured and combined in an and/or relationship.

9.12.3 Upgrade rules

Upgrade rules are triggered when a client want to upgrade his current package. This happens when they enter the upgrade domain in their browser e.g. <http://upgrade.com>. The upgrade rules are identical to the standard rules but they only have the option to specify the billing packages. There is also an additional trigger, the current billing plan of the subscriber.

9.13 Walled garden

9.13.1 Introduction

IP addresses / domains or URLs in this list will be accessible for all subscribers in this subscriber network selected without authentication.

9.13.2 Simple configuration

- IP / domain: can be an IP (1.2.3.4), IP/netmask (1.2.3.4/24) or domain (fdxtended.com). To allow all subdomains you can use *. like *.fdxtended.com
- Port: optional
- Protocol: all, udp, tcp and icmp
- location: specify the location the walled garden should be applied, guest networks without location will also be used when "all" is selected

9.13.3 Advanced configuration

The advanced configuration supports regex, path and action (allow / disallow) but due to performance penalty we recommend using the default configuration.

10. System

10.1 Introduction

All system wide tools like:

- backup
- Performance
- Language
- Theme
- ...

10.2 Access control

10.2.1 Settings

In access control you can add administrators for the gateway. The person logging on will have access to certain parts of the system depending on the username that they log on with.

In this section you can choose how users can authenticate

- Internal: administrators can only use a valid username/password in the internal database (see users tab)
- Internal and LDAP: the system first checks the username/password with the internal database, if this fails the gateway will connect to the LDAP server and start a search for this

username. If one matches we look at the LDAP rules (see Access control rules tab in ldap settings) to see which rights belong to this user. If a rule has been found the system will grant access to the gateway.

Note: The LDAP configuration should be done in Periphery- LDAP settings.

10.2.2 Users

This is a list of internal administrators. You can add an administrator by clicking the add icon. To change or delete an administrator you can use the commands in the action column.

There are 2 different administrators, regular administrators and pos users.

Regular administrators

These users will have access to the normal interface and all pages which are selected in their profile. To enable all pages you can simply use the superuser checkbox.

POS

POS users have a limited login, they can only add users and manage their own created user profiles. When a POS administrator creates an account, a ticket will automatically be opened in a popup so that this can be printed.

You can configure the type, billing packages, required fields, pos content and rights of a POS user by clicking the add button and enabling the POS checkbox. It's also possible to link an administrator to a group profile. The rights of the group profile will then be triggered instead of the rights of the individual users.

10.2.3 Groups

Administrator groups contain a preconfiguration for an admin account. When an admin account is tied to a group it will take over the properties of the group so it is easy to quickly add an administrator based on a group. These groups are also used to link LDAP administrators to their properties (see LDAP rules).

10.2.4 External users

This is a list of users that connected with the LDAP plugin.

10.3 Factory reset

The factory reset module allow you to reset the HSMX to factory standard. The factory can be done partially so for example if you do the factory remotely that you do not lose Ip connectivity after the reset. (by unchecking the Reset network configuration option)

10.4 System language

To change the language, click on the language of your choice.

The gateway gives you the ability to create your own language, every page can be translated separately which makes it possible to just translate the pages that you need and leave everything else standard (English).

To enable this feature you have to enable the language update. If you enable this functionality a globe will appear on every page.

You can also go directly to the translation page by clicking on the language name.

10.5 License

On this page you can see the license and the enabled modules. It is possible to request a 30day demo automatically by clicking the link next to the module you want to demo. In case you bought a module or user upgrade, you need to renew your license. Just press the "get license key" button to get your license key.

Enter license key manually, is only needed when support gave you a big license string to recover your license because no access to our license server is possible.

10.6 Login screen

Here you can update the layout of the admin login screen of the gateway.

You can also add a partner image (jpg only) that will be shown above the login box.

10.7 System Performance

10.7.1 Introduction

The performance module of the HSMX allows you to tweak system services / settings to achieve better performance.

The defaults provided are fine in almost any case but in some circumstances (very large networks / many portal redirects) some of these settings can be changed to achieve a better response time.

10.7.2 Configuration

Portal redirect

In this section you can tweak settings related to the portal redirect. The portal redirect is one of the most CPU intensive tasks there is, mainly because there are so many. Each http request from

a pending client is forwarded to the portal, this section is really important if you have many devices in your network that are pending (not logged in). The problem is that 90% of the redirects are generated by background services, not a client opening the browser. All these background services setup a http request to update a service on the Internet. Some examples of these services are virus scanner updates / OS updates / toolbars / viruses / Social media apps /

Disabling unneeded services can help deal with the large number of portal redirects.

- Roaming: Enable or disable a check that a client is roaming from one subscriber network to another.
- MAC redirection: Enable or disable a check whether the redirect originates from a device in the MAC list.
- AAA: Enable or disable a check where we verify if the request comes from a location that has AAA disabled.
- Pre-portal: Important Show a redirection page before the actual portal to exclude fake browsers from hitting the real portal page. This will decrease the load of the web server making room for real browser redirects.

web server

Here you can tweak the web server settings, this is also important when the system is put under load with many portal redirects. If the system becomes too slow it may be needed to set the max server processes to a lower value, this means the web server will accept fewer connections. But setting it too low may cause the web server to respond slowly because all connections are used up but the server could not be under load at all. Important to check the CPU load before changing this setting (system => task manager). The keep alive setting also has a big impact on the system and also on the max server process setting. Keep alive means that a connection is kept open to transfer multiple files quicker rather than opening a new connection for each file. When there is no load, keep alive can speed up portal display. Just make sure that you also increase the max server processes because much more connections will be open all the time. When the system is under a lot of load by many pending users, it is recommended to disable the keep alive because almost 90% of the redirects are background services, they will use up all the available connections because they are kept open for as long as the keep alive timeout.

database

You can tweak the memory consumption and the amount of connections that can be setup to the database. Giving the database more resources can be interesting when the user database is very big. It is possible to verify memory usage of the system via the health widget in the home screen. Based on this information it is possible to give the database more memory. Do this only when the system becomes slow.

PHP

In this section you can change the upload file size. if you have to upload large portal pages or large system backups it may be needed to increase these values.

connections

expert only

Here you can tweak settings related to TCP/IP handling. Only change these values when you know what they mean or when instructed by support. When using multiple public ip's, it is needed to increase the `nf_conntrack_max` value to $64000 * \text{the amount of public ip's}$. At least when these public ip's are used for natting.

Content filter

In this section you can adjust the content filter (if licensed). It's best to increase the amount of `maxchildren` to the amount of licensed subscribers.

Maintain roughly the same ratio between the values as they had with their default values.

10.8 System settings

System mode

- Gateway: default mode, when the client will contain subscriber networks
- Authentication: when the gateway will serve as authentication gateways without having guest networks
- Mixed: when the gateway has guest networks and is also authentication server for external guest networks

License mode

- Per device: default setting, user license is counted per active device
- Per room: User license is counted per room. Bandwidth is shared per room account. Room license counts per subscriber networks.

SMTP settings

This are the settings the system will use to send e-mails (welcome e-mails, status alerts,...). SMS settings have their own SMTP settings.

Health reports

Sends a status of the system health in case the system went from healthy to unhealthy or the other way around. A threshold can be configured so the gateway will only send an e-mail when the device has the same critical/warning status a few times in a row.

Deprecated mode

Some features have been replaced by other functionalities. You can hide all deprecated features by disabling this feature.

Some features that have been replaced are:

- Billing -> free access, can now be found under the extra menu and be enabled in the portal rule.
- The HSM portal, this feature has been replaced by the portal editor.

Admin idle timeout

The device will throw a message if it doesn't detect any activity of the administrator. The user will then be logged out after 10 seconds if he ignores the message.

System menu

Show the submenu based on hover or click.

10.9 System backup

10.9.1 Introduction

System backup is a set of tools to backup / restore / clean (log files) / remote backup the system.

FTP location

In case you want to upload your backup to an external FTP server configure a FTP location.

10.9.2 Backup

The gateway can perform an automated backup on the requested interval. The gateway doesn't store more than 10 backups, older ones will be removed. If the FTP is configured, you can upload the backup to the external FTP. By clicking the backup now, the system will start to backup right now.

10.9.2 Log handling

In log handling you can clear out older log files.

Log files are stored in a archived format (for download) and in a text format for review via the GUI. The log files in text format take up a lot of space so it is important to remove the log files

regularly (e.g. every 4 weeks). The log archives can be stored a bit longer but should eventually also be removed. There is always the option to upload the log files to an external FTP server.

10.10 System updates

When an update is available, the system will prompt the user about the upgrade when the administrator logs in.

To check manually, go to system => updates and click check updates now.

When an update is available, click on install and the new firmware will be installed.

10.11 Time settings

The gateway syncs with NTP time servers to keep the time up to date. Enter the correct timeservers, timezone and apply to confirm and sync the time.

11. Security

11.1 Introduction

Security related features such as the firewall, intrusion detection and SSL.

11.2 Firewall

11.2.1 Introduction

The firewall module protects the system services from exposure on the Internet. The firewall rules can be ip or subnet based so the services are only opened for those who need it.

Note Be careful when changing the firewall rules to avoid locking yourself out from the web interface.

11.2.2 firewall rules

Description: Descriptive name for the firewall rule

Ethernet interface: The Ethernet port this rule needs to be applied to.

Direction: Incoming packets (default), outgoing packets (packets generated by the gateway itself, not subscriber traffic).

Protocol (All / TCP / UDP / ICMP)

Action: Accept / Reject (sender will know the service is blocked) / drop (dropping the packet without confirmation)

State: All / Established (existing open connections) / Related (related packets e.g. ftp-data)

Port: TCP / UDP port the rule applies top (Unless any port is allowed)

Source IP: IP address / subnet of the sender

Destination IP: IP address / subnet

11.3 Intrusion detection

11.3.1 Introduction

The intrusion detection module safeguards the system by actively blocking or warning when brute force log-in attempt is done.

The system can block access to the web interface for a configurable period when too many log-in attempts are done.

it is also possible to move the ip of the offender to the blacklist and at the same time warn the admin about the event.

The system has ip based access control, either we accept every IP except the offenders listed in the black list or we block every IP except the ip or ip ranges listed in the white list. If you don't want subscribers to gain access to the admin GUI, you can put the LAN subnet in the black list as well.

11.4 Log settings

11.4.1 System log

Enable the logs you want to see in the log menu. You can also send the logs to a external syslog server by filling in the syslog server field.

11.4.2 lawful interception

Choose if the device needs to log user activity and specify what details need to be stored. You can send the logs to a remote server by enabling remote logging.

URL logging

This setting will use an internal proxy server to log all URL's from online subscribers. Only use this feature if it is allowed to log this information in your region.

Using a proxy removes some functionality like QoS for web traffic or one2one natting. URL logging will not work when the client sets up a VPN connection.

11.4.3 reports

This module generate the reports which can be viewed in extra - reports and feeds some widgets in the Home screen.

VLAN report can be activated separately because this can decrease system performance when you have a lot of VLAN's.

11.5 Network policies

Network policies is in fact a client firewall, these rules are read from top to bottom until 1 rule is triggered.

To apply a network policy you can assign 1 rule or group to a location or billing.

With a network policy, you can manipulate the subscriber traffic.

- Drop
- Accept
- Limit packets
- Limit connections
- Redirect

You can do these action based on traffic type (TCP (+port) / UDP (+port) / ICMP and / or on a destination ip / subnet.

You can group network policies by checking them and clicking the "add to group" link, this is needed if you want to apply multiple rules at the same time.

11.6 SSL

10.6.1 System SSL

With this module you can manage the SSL certificate of the webserver. Standard the system is loaded with the certificate login.fdxextended.com, this is a valid certificate.

In case you already have a certificate, you can use the enter SSL certificates manually. You can input the private / public key and the CA certificates.

in case you still need to generate a certificate, click on generate CSR to create a certificate signing request, with this CSR you can buy a SSL certificate with a known certificate authority.

10.6.2 Guest networks

If a valid SSL certificate is uploaded you can enable the following options:

- Redirect portal requests to HTTPS: all portal requests will use HTTPS
- Support HTTPS redirections on the LAN side: by default the gateway doesn't accept HTTPS request for non-authorized clients, by enabling this feature the portal will also be shown for HTTPS request although an invalid SSL certificate warning will be shown by the browser.

12. Tools

12.1 Introduction

A selection of tools that can be used to troubleshoot, generate reports or download logs.

12.2 Bandwidth report

The bandwidth report module displays real time bandwidth usage. You can specify the desired network port from the dropdown.

Th download / upload bow is to see the report for either the incoming traffic or outgoing traffic.

12.3 Connection test

Ping

See if the device is able to ping an external host to verify the network connection and if domains can be resolved.

TCP connection

Test if the gateway is able to connect to a specific IP and port.

12.4 Download log

The download log module is there to download the log archives, the log archives are created on a daily basis. Alternatively you can also have the logs uploaded to an external FTP server.

- Syslog
- LAN Syslog
- FIAS log
- Lawfull interception
- URL log
- Credit card

12.5 Interface status

This graph displays the status of the interfaces in the system based on the link status and monitoring configured in network settings.

Specify the date of the report, and press show.

Tip When you go over the graph with your mouse it zooms in.

12.6 Logging

Here you can see all the system logs. The logging is useful for troubleshooting purposes.

There is an advanced search option in the logs. You can select the hour, facility and level you want to filter on.

You can also search a specific word in the log files. You can use regular expressions (helper available) when you do a search on a specific word.

There are several logs available:

- Syslog

Global log of the HSMX including portal events.

- LAN Syslog

Logging of the individual subscriber networks

- XML log

XML log is the communication log between an authentication system (or UMS) and the HSMX.

- FIAS log

FIAS log is the communication log between the HSMX and the PMS system. It is also possible to download the FIAS log of the current date.

- Payment log

Payment log is a list of all payments that have occurred (PMS / credit card)

- Lawfull interception

Lawfull interception will show all connections of a user for legal reasons.

- URL logging

URL log is a list of the visited websites (only when the module is enabled) (see log settings)

12.7 Packet capturing

With this tool you can take a packet capture on any interface.

Use the filters to have a capture that only contains the results you are looking for.

The option save to file stores the capture in a PCAP format readable by most packet capture software.

12.8 Portal debug

Portal debug is an advanced debugging feature of the portal page sessions.

Since the portal debug generates so much data it is important you only enable it when you are debugging a specific issue that is guest related.

The log shows you the exact user input and all the variables that are active at the time a guest is logging on.

12.9 Reports

12.9.1 Graphical reports

Reports that are displayed in a graph, most of them can also be found as widget.

Some graphs will display an excel icon, clicking this icon will generate an excel file of the generated graph.

12.9.2 Report

Create a report based on bandwidth utilization, subscribers or revenue.

12.10 Task manager

The task manager lists the HSMX most critical services and background scripts.

By using the action link on the right side of the service you can (re)start or stop the service.

The task manager also gives a clear picture of memory and CPU usage of the system. In case you get a blank page, increase the refresh rate.

13. Periphery

13.1 Introduction

All the modules related to external applications / tools / devices and interfaces.

13.2 Account printer

13.2.1 Introduction

Account printers are 3 button printers to easily generate and print vouchers.

13.2.2 Configuration

Make sure the printer is configured correctly and is able to contact the gateway.

Enable the service, choose the correct port and fill in the printer IP.

Add this port to the firewall, otherwise the device will not be able to talk to the gateway. (See firewall)

If the printer is connected from the LAN side you have to activate it first. (see Activate subscriber)

You can simply add or edit a printer by pressing buttons. You need to configure the printer IP and how many times a voucher needs to be sent to the printer. To configure a printer button you can press one of the button icons.

13.3 Client gateway

13.3.1 Introduction

When the system is running in authentication or mixed mode you can let external guest networks join this gateway. This gateway will act as authentication server while client traffic is still handled by the external gateways.

13.3.2 Configuration

Add the IP address and login credentials of the gateway holding the guest networks you want to add. If the gateway is added and connection towards the device is successful you will see an additional icon to view all guest networks.

Check the guest networks which should redirect clients to this gateway for authentication and press save. The joined guest network will now redirect all clients to the IP address which was used to reach the external gateway. This IP address can be viewed/changed by going to network

-> network configuration -> click edit on the guest network -> virtual section on the external gateway.

13.4 Credit card settings

13.4.1 Introduction

The gateway is compatible with a range of credit card clearing houses and paypal, these services can be used to automatically charge for Internet access without any other user intervention. The client can buy a package for the price configured in the billing plan and will automatically be logged in afterwards.

Note: The credit card option will only be available on the portal page when credit card or paypal is enabled in the payment section of the portal rules.

13.4.2 Credit card service

This feature is depreciated.

13.4.3 Credit card module

There is an option to enabled or disable the (optional) module. The option invoice allows the client to receive an invocie for the payment via e-mail. See general settings for more configuration options.

The gateway is compatibel with several credit card clearing houses. Select the credit card clearing house from the drop down list.

There will be several configuration option that need to be entered depending on the chosen clearing house. These details should have been supplied to you by the clearing house.

13.4.4 Paypal

13.4.4.1 Introduction

Paypal is a popular payment service, clients can buy packages with their paypal account or also without paypal account and just a credit card.

13.4.4.2 Configuration

- PayPal URL: URL that is being used to contact PayPal (www.paypal.com/cgi-bin/webscr)
- Merchant ID: Your PayPal e-mail address

- External IP: The WAN IP of the device, without this PayPal cannot contact us and we cannot verify the purchase.
- Return button: Text that will be displayed on the return button.
- Currency

13.4.5 Add your own clearing house

Instead of using one of the predefined clearing houses you can add your own, an API of the clearing house is required to know the exact flow and variables. The following can be configured:

Submit fields

This is the form that will be sent to the clearing house (and also the customer redirection to the payment page). All values (operator applied!) are saved and can be used in the clearing house answer.

|| characters are used for variables generated by the system, these can be ||portal_url|| (example: http://login.fdxtened.com), ||order_id||, ||amount|| and ||currency||. % characters can be used for variables created in this section (including the operation), for example %AMOUNT%, in order for this to work AMOUNT has to exist (field name) in one of the rows above.

For example if row 1 would use field name "AMOUNT", operator "*100" and amount is "10", you can use from row 2 onwards %AMOUNT% which would be "1000" (10 * 100).

Answer

The answer is the status of the payment that is being sent from the clearing house to the gateway. This answer should be returned to https://[gateway public IP]/creditcard/cc_notification.php, it is possible this URL needs to be specified in the submit fields or in the clearing house settings, without this URL the payment will never be approved.

Order identification

An unique Id has to exist to match the submit fields (request) and answer, therefore the orderId has to be in the submit fields so the clearing house can return this value in the answer. Here you can specify in what variable the clearing house sends back the orderId.

Flow

The flow is how the system will check the incoming answer and can be fully customized. An incorrect check however can lead to creation of accounts while payments were rejected.

% characters are being used to indicate return variables from the clearing house, for example %amount% || characters are being used to use variables that were sent to the clearing house (the ones created in Submit fields including the operation), for example: ||amount||

13.5 LDAP settings

13.5.1 Introduction

The LDAP (Lightweight Directory Access Protocol) module allows the system to connect to an external LDAP server to authenticate administrators and subscribers.

13.5.2 LDAP servers

In this section you can add / update and delete LDAP server connections.

13.5.3 Access control rules

This are the rules that will link a group profile to an external administrator. The rules are being read from top to bottom so the first rule that matches will be applied. You can change the order by dragging the number in the sort column.

Default

If enabled, this will become the default rule, a default rule will always be matched so it's recommended to add this as a final rule.

Attribute

This is the attribute that will be returned by the active directory so we can compare the value.

Match

If this value matches the attribute value, we apply the group that is linked to this rule.

Group

Group that will be used when this rule is applied.

Example

Attribute: ou
Match: pos
Group: group1

If the returned attribute (ou) matches "pos" we will login the administrator with the rights of group1

13.5.4 LAN rules

This section is identical to Access control rules besides the fact it used to authenticate subscribers rather than administrators of the system. When a subscriber authenticates, depending on the rules, a package will be created with the configured billing plan.

13.6 PMS settings

13.6.1 Introduction

The PMS module is an optional module of the system. It connects the gateway to a PMS (property management system), this way the gateway retrieves all guest details of the hotel and it can also charge the guest folio.

13.6.2 Configuration

13.6.2.1 PMS type

- FIAS serial (basic)
 - This enables our basic PMS interface
 - Guests can be authenticated on any field in the PMS
 - No support for sharing guests
 - Uses the serial port to connect to the PMS system
- FIAS IP (basic) - This enables our basic PMS interface
 - Guests can be authenticated on any field in the PMS
 - No support for sharing guests
 - Uses the network (TCP) to connect to the PMS system
- FIAS serial (advanced)
 - This enables our advanced PMS interface
 - Guests can be authenticated on any field in the PMS
 - Support for sharing guests
 - View bill on the portal page (portal page must support this)
 - View text messages coming from the hotel staff (portal page must support this)
 - Check out on the portal page (portal must support this)
 - Uses the serial port to connect to the PMS

- FIAS IP (advanced)
 - This enables our advanced PMS interface
 - Guests can be authenticated on any field in the PMS
 - Support for sharing guests
 - View bill on the portal page (portal page must support this)
 - View text messages coming from the hotel staff (portal page must support this)
 - Check out on the portal page (portal must support this)
 - Uses the network port to connect to the PMS
- FIAS agent (basic)
 - This enables our basic PMS interface
 - Guests can be authenticated on any field in the PMS
 - No support for sharing guests
 - Connects to the agent instead of directly to the PMS
- FIAS agent (advanced)
 - This enables our advanced PMS interface
 - Guests can be authenticated on any field in the PMS
 - Support for sharing guests
 - Connects to the agent instead of directly to the PMS
 - View bill on the portal page (portal page must support this)
 - View text messages coming from the hotel staff (portal page must support this)
 - Check out on the portal page (portal must support this)
 - Connects to the agent instead of directly to the PMS
- OnQ
 - OnQ interface (similar to FIAS IP BASIC)
- Amadeus
 - Uses Amadeus interface (Similar to FIAS IP BASIC)
- UHLL
 - Universal Hospitality Language Layer from control

Note The option use all definable fields, set the system parameters so all 10 user definable fields that are available in the FIAS specification can used instead of the standard 2. User definable fields can contain any value that is available in the PMS to be used for identifying the guests (e.g. loyalty membership number).

13.6.2.2 Logical settings

You can select the fields that the guest has to enter to authenticate. We have 3 sections, room known (and checked-in), room unknown, room shared.

- room known

This is only triggered when there is a vlan per room and the system can identify what room the client is connecting from. If no fields are checked, the client can get online without any further authentication.

- room unknown: This is the most frequent scenario, the system doesn't know beforehand where what room the client connects from so the first mandatory field that is requested is room number. check one or more fields to make the authentication more secure.
- room shared: When 2 or more people share a room, the gateway identifies these as separate guests that need to be individually charged and authenticated. Enter the fields that ensure the authentication is unique e.g. combination of first and last name.

No post options

It is possible to ignore the no-post flag of a guest by enabling this option. Keep in mind a no-post flag means there is no credit card available to recover the charge in case the guest would not check-out. Alternatively, it is possible to ignore the no-post flag only for free access billing packages since there is no charge involved.

13.6.2.3 PMS field policies

Here you can specify how strict we check the input of the guest against the PMS database. This overcomes problems when the front office types the guest name wrong or when special characters cause problems with the input.

You can create multiple policies and you can assign a policy per PMS field and / or set a default policy for all fields.

Examples

- Match 4 characters beginning
- strip space / dash / Quote

PMS database, guest name: O' Donald => stripped to: odonald

Guest input, guest name: O'donnald => stripped to odonnald

Match because: **odonald** => **odonnald**

4 characters matched in the beginning of the guest name

13.6.2.4 Connection

Depending on the selection in the first tab you will see different options here.

Send ACK

- Only required for serial connections
- Send acknowledge after every message received
- Wait for acknowledge after every message sent

Send LRC

- Only required for serial connections
- Send a check-sum with every message sent
- check check-sum for every message received

Send LA

- Send link alive message every x minutes

Database swap

- Every X minutes a database swap command will be sent, this is not recommended because a database swap can take a long time and during this swap no postings can be sent to the PMS.
- Fixed hour: This is recommended.
- On start: This is also a recommended setting.

Sanity check

This option will determine if the device needs to wait for a link alive check from the PMS when the device sends a link alive itself.

Send billing name / fixed variable in charge

This will fill in the CT field when posting to the PMS.

Buffer charges

When a guest tries to charge his room he has to wait until we receive an acknowledge from the PMS before he is able to browse. Or if the PMS is down the client will get an error message that he cannot charge his room at this time.

To bypass this you can simply buffer the charges, this way clients don't have to wait and will go straight online. Our PMS interface will take care of all charges and will send them to the PMS system as soon as possible.

Warning message

In case when there is no communication for a certain period, the admin will be notified by e-mail. This setting will use the SMTP settings configured in system -> system settings.

13.6.2.4 Agent

An agent can be configured to forward all incoming guest data to an external authentication system.

There is a listener and a sender, the listener waits for requests while the sender sends updates whenever we receive an update from the PMS.

Communication can be encrypted.

13.7 RADIUS profiles

Configuration of the different RADIUS profiles.

The RADIUS profiles can be configured in the subscriber (LAN) network in the AAA section (see AAA)

Name

Name of the RADIUS server

Type

(PAP - CHAP - MS-CHAPv1/2)

Authentication server IP

IP address of the RADIUS server

Authentication server port

Port used for the RADIUS authentication requests

Accounting server port

Port used for the RADIUS authentication requests

RADIUS secret

Secret for communication between this NAS and the RADIUS server.

NAS identifier

Identifier to identify the connection of our subscribers on the RADIUS server

Timeout

Amount of retries

Overwrite WAN IP (optional)

This will disable the auto detection of the WAN IP in the RADIUS requests made.

MAC (needed if WAN IP is used)

MAC address of the system, can be found in Network configuration.

13.8 SNMP

Enable SNMP when you want to retrieve certain OS values from the system.

The gateway can send traps on certain system events, MIB for the SNMP traps is available in the web interface as download.

13.9 UMS

UMS or User Management System is a free Windows based program to create vouchers. You need to enable the UMS server here to make sure the program can contact the gateway.

You can choose to allow all IP's or just a few. Only these IP's will then be able to use the UMS server.

For more information, check out the UMS manual.

13.10 XML server

If you want to make use of the internal XML server you need to enable this here. You can also choose if you want to allow all IP's or just a specific IP address. Only these IP's will be able to send

XML commands to the gateway.

The RADIUS override allows you to override the standard RADIUS settings and use the RADIUS server configured in the configuration.

Contact support for the XML API.