1. HSMX 4.7 manual

1.1 Introduction

The HSMX gateway is an internet access solution. It is suitable for small to very large networks and for free / charged or mixed internet access.

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

- User management

- Portal page

- Billing packages

- Settings (system / modules)

- LAN (subscriber networks)

- (WAN) network settings

- Reporting

Configuration over the web interface. There is a limited serial interface to perform a factory reset / admin reset or ip change.

1.2 Initial setup

1.2.1 Introduction

The first time configuration can be done in 3 ways,

- serial

- connected to the LAN port (DHCP)

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

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

1.2.2 serial

Connect to the serial port with a NULL modem cable with the default settings (speed=9600,Data 8bit, stop bits 1, no parity, no flow control).

- Press enter

- Log in with password manager.

- ipconfig eth0 ip_address subnet (replace ip_address and subnet with the correct ip address and subnet).

After that connect with a webbrowser to the ip address configured and log in with admin / admin.

1.2.3 connected to the LAN port (DHCP)

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 http(s)://192.168.80.1 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 http(s)://10.10.10.1 and log in with admin / admin.

1.2.5 next steps

Go to network => network configuration and configure the network settings for your network.

2. Home Screen

2.1 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:

- Statistics
- Health monitoring
- Subscriber networks
- Locations
- Bandwidth monitoring / throughput
- User history
- DHCP lease usage
- User license usage
- Room occupancy (in combination with the hospitality module)
- Log (latest events)
- Update notifications
- Packets
- Revenue
- Filter / portal redirects

2.2 Usage

To activate the widgets, click on the jigsaw icon in the navigation bar. 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.

2.3 Locations

2.3.1 Introduction

One of the widgets is the locations, locations are logical divisions inside your property. The divisions are separated by vlans / subnets or LAN port.

Locations can be used for statistic reasons but also for logical configuration. It is possible to show a different portal page per location, or restrict a user account to a single location. This means a voucher can be valid in location 1, but as soon as they roam to a different location, they need to reauthenticate with a voucher valid in the new location.

2.3.1 Configuration

First of all make sure you have the location widget visible in your home screen. To add a new location, press the building icon in the navigation bar () and enter the logical name of the location. Now the location will be listed in the Location widget. Press the update icon () to update the location. Now you can specify the subscriber network and vlan or subnet you want to use for this location, multiple vlans / subscriber network or subnets can be used. There is a AAA section for the location, here you can specify if you want free / open or charged service on this location.

- Charge: Users will be redirected to the portal page.
- Open: Users will be redirected to the the Internet.
- Close: Users will not be able to go online in this location.

In combination with the QoS module of the HSMX it is also possible to set a default QoS profile for clients connecting in this location. The QoS profile configured here has a low priority so it can be overridden by the QoS profile setting in the client profile.

2.4 Subscriber networks

This widget gives you access to the subscriber networks, a subscriber network is the configuration of the client network. The design of the HSMX allows you to have multiple subscriber networks, each with its own configuration. A subscriber network can be tied to a physical LAN port or to a VLAN configured in the network settings. The widget is a strategical overview but all the functionality is accessible through the LAN menu as well. For more information see the LAN section of the manual.

2.5 Statistics

In this widget you can see the amount of subscribers divided in different categories:

- Active subscribers
- Pending subscribers
- Idle subscribers
- Expired subscribers
- Unused subscribers
- Blocked subscribers

2.6 Monthly statistics

In this widget you can view the overall usage of this month, this data is gathered from the user database and is only populated when reports are enabled. (see log settings)

- Data transferred up
- Data transferred down
- Total revenue
- Subscriber sessions

2.7 Health

This widget is used to monitor the status of the gateway, it has several sections:

- General: this is a report of the status of all different services and Ethernet ports.

- Disk space: Here you can monitor disk usage, when free space is getting low, it is recommended to configure log handling so old logs are purged. (see system backup (log handling))

- Connections: This displays the number of connections setup in the system, these are mainly generated by natted client connections. It is possible to tweak the maximum allowed connection and TCP timeouts in System performance.

- CPU: Diplays the CPU usage, if load is too high, it is possible to tweak the system in System performance.

- Memory: displays memory usage, keep in mind the system will automatically cache data so it is normal memory usage is not very low.

Note Whenever a Calendar icon (📅) is displayed on the top right of the icon, you can click it and go to a full page view of this widget where you can sort on date, period and backup the data.

2.8 User history

This widget shows the amount of users connected to the system, this also takes into account users without authentication (AAA) enabled, external authenticated users and internal authenticated users. Click on the Calendar icon to get the full page view of the report including more filter options.

2.9 Bandwidth report

This widget shows the bandwidth usage on the network interfaces., these are averages over 2 minutes. Click on the Calendar icon to get the full page view of the report including more filter options.

2.10 User license

This widget shows the usage of the user license. It will display a percentage of what is currently used of the user license.

2.11 Update

This will display the availability of an update and the status of your maintenance contract, you can update to a new major release when a maintenance contract is in place.

2.12 Packets

The number of subscriber plans created.

2.12 Revenue

Based on bought billing plans.

2.13 Filter / portal redirects

See how many non-active devices are hitting the portal page or a specific filter.

3.0 User management

3.1 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.

3.2 Subscriber overview

Introduction

This module shows all users in the user database, 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 (⧉), 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.

Sections

- Active: Subscribers/Vouchers that are currently logged in.
- External: This tab will show all users that are logged in on an external radius (only visible when external radius is enabled).
- 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.

3.3 Subscriber Search

3.3.1 Introduction

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

3.3.2 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 (username which was last seen with this MAC will be displayed)
- All 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 icon (ℹ) next to the subscriber to update or view the details.

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

3.4 Subscriber Profile

3.4.1 Introduction

After clicking on the subscriber details either in the subscriber overview or the search module, you see the details of the subscriber package.

The overview page has 2 sections, the first section is the overview of the packages tied to this subscriber. A single subscriber can have multiple packages, when the first package expired, the same subscriber (user name) can be used to buy a second package. It is also possible to upgrade the package, either the subscriber can do this on the portal page or the admin can do this by selecting a new package in the drop down on the top left. The values are initialized by the billing plans, but all values can be changed after the subscriber is created.

The second section contains the account details, here you can find personal information about the account (when available). This is populated by the administrator who created the account or by the subscriber itself with auto registration on the portal page.

3.4.2 package details

The package details show the limitations set for this subscriber, the left column represents the current package of the subscriber, packages on the right are previous packages. In the header of each column, you can see the package name, how it was purchased (voucher / credit card / PMS (hospitality module)), and when it was bought. Below you can see an overview of all listed settings:

- 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

- 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.
- Calender days: The account is only valid on the days /hours specified in this calender 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 to 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 expired, usually initialized after first login.
- Delay expiration, if the package has the option set to expire on guest checkout (Hospitality module) a timeout can be set so the account is still valid for a few hours after checkout.
- Accounting Interim Interval: interval on which the profile is updated with the latest data / time usage.
- 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.

3.4.3 Account details

The account details contain the personal information tied to this subscriber profile such as address / phone, ...

3.4.4 Update

In this section you can update all values. When the account is active at the time, these settings will be applied to the active session immediately.

For an explanation of the option see above.

3.4.5 Active sessions

This produces a list of all current sessions of this subscriber profile. The list displays the start date data volume used, mac, IP address and subscriber network . The frequency of updates depends on the accounting interim setting in the package.

3.4.6 Non-active sessions

This produces a list of all past sessions of this subscriber profile. The list displays the start and end date, data volume used, mac, IP address, subscriber network and termination cause. The sessions are grouped per subscribed packages.

3.4.7 Lawful interception

This is a list of all connections of the client, only populated when the lawfull Intercept module is enabled. (See log settings)

3.4.7 URL logging

This is a list of all visited web pages of the client, only populated when this feature in the lawfull Intercept module is enabled. (See log settings). This setting can depreciate performance of the web connections as all these connections will be forced through a proxy server.

3.5 Add subscriber

3.5.1 Introduction

This module is designed to add a single subscriber to the system.

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

Note You can Also create your own "add subscriber" interface by creating a registration form, make it visible for the admin interface and assign it to your admin rights.

3.5.2 Use

- Enter the fields or press the 🔄 to generate a username / password or voucher code automatically.

- Specify a template so the voucher can be printed and given to the client. (for more info see Templates)

- Specify a billing package with the limitation for the voucher.

3.5.3 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.

3.6 create vouchers

3.6.1 Introduction

This module is designed to add a batch of subscribers to the system.

Depending on system configuration (see general settings - voucher code only) a user name / password combination is created or only a voucher code.

3.6.2 Use

- Enter the amount of vouchers that need to be created.

- Optionally a prefix can be entered so the user names all start with the same prefix.

- Specify a template so the vouchers can be printed and given to the clients. (for more info see Templates)

- Specify a billing package with the limitation for the vouchers.

3.6.3 Advanced settings

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

- Specify voucher or CSV, in case the vouchers need to be exported to a CSV for printing, chose CSV and specify the CSV option below. In case printable voucher templates need to be created, specify voucher.

- Choose alphanumeric / numeric or combination for the generated access codes.

- Optionally enter a company name and tie the generated accounts to a subscriber group.

- 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.

- Amount to print, this option will print the created account X times in the template.

3.7 Insert (import) subscribers

3.7.1 Introduction

The insert subscriber module can be used when vouchers have already been generated by another system. When they are available in CSV format they can be imported here.

3.7.2 Use

When you have a CSV file with user names and passwords, verify the format of the CSV file, either the fields are separated by a comma "," or they are separated by a dot-comma ";". Specify the billing package where the imported codes need to be created with.

Note When the system is configured with voucher code only (see general settings - voucher code only), the user name and password that is imported should be identical.

3.7.3 Customize CSV

It is possible to specify the order of the columns and to include other fields then user name / password.

3.8 Insert MAC address

In this module you can quickly add a MAC address to the user database. When a device connects to the network and the MAC address of the device is listed in the user database, the device can immediately go online without authentication. When a MAC address is added with status disabled, all traffic of this device will be blocked. You can change the status of a MAC based subscriber anytime by editing the account. All MAC based users can be found in Subscribers overview - mac list. The username can be put in so you can name the device you entered.

3.9 Insert (import) MAC list

3.9.1 Introduction

The insert MAC list module can be used when you have a list of devices (MAC addresses) that need to get connected without authentication. When they are available in CSV format they can be imported here.

3.7.2 Use

When you have a CSV file with the MAC addresses, verify the format of the CSV file, either the fields are separated by a comma "," or they are separated by a dot-comma ";".   You can assign a tag to these MAC addresses so you can easily remove them by their tag id in subscribers overview.

3.10 Create SMS subscriber

In this module you can create subscribers based on their mobile number. Standard the mobile number will be used as username and the password will be sent to the entered phone number. Unless the option is unchecked, a username will be generated. All SMS settings including the billing plan need be configured in settings -> SMS settings.

! SMS settings are depreciated, create SMS subscribers can be replaced with registration forms.

3.11 Activate subscribers

3.11.1 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.

3.11.2 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 then creating a new one.

3.12 Voucher list

This lists the generated 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.

3.13 reload cards

3.13.1 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:

  - Numeric
  - Alphanumeric
  - Numeric / alphanumeric

- Number of characters

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

3.13.2 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. Settings

4.1 Introduction

The settings menu is used to configure options for several (optional) modules.

- General settings

- Billing settings (Hospitality module / credit card)

- Account printers

- ...

4.2 General settings

Settings related to the entire system..

General
Name: The site name.
Currency: Currency that will be used for the billing plans, currencies can be created in extra -> currency (see currencies).

Account warning
These are warnings that will be showed to the customer if his account is running low on time or volume. This only works if the logout console is still open, if the logout console is disabled or the customer closes the logout console, no popup warning will be given.

Postmaster (hospitality module)
This setting will post a charge to the PMS system when an account is created or when the account is being used for the first time. (this is the case for add subscriber, create vouchers, subscribers created by the account printer,....)

Password policy
You can select the password policy that applies to this site, this only counts for subscribers, not for administrators.
See extra -> password policies for more information.

Voucher code
This setting will disable the password field so that subscribers can login with just their username (voucher code only). This setting will apply for all portals and when creating vouchers.

Free access account reset
Here you can choose when users that got free access are eligible for free access again.
This is only valid for free access created in billing -> free access.

E-mail content for credit card invoice
E-mail that will be sent to the guests when paying via credit card.
This option has to be enabled in credit card setting.

4.3 Account printer

4.3.1 Introduction

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

4.3.2 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 send to the printer. To configure a printer button you can press one of the button icons.

4.4 Credit card settings

4.4.1 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 (see rules).

4.4.2 Credit card service

This feature is depreciated.

4.4.3 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.

4.4.4 Paypal

4.4.4.1 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.

4.4.4.1 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

4.4.5 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.fdxtended.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 exists 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 specifiy 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||

4.5 PMS settings

4.5.1 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.

4.5.2 Configuration

4.5.2.1 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 comtrol

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).

4.5.2.2 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.

4.5.2.3 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: **odon**ald => **odon**nald
4 characters matched in the beginning of the guest name

4.5.2.4 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.

4.5.2.4 Agent

An agent can be configure 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.

4.6 Log settings

4.6.1 System log

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

4.6.2 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.

4.6.3 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.

4.7 SMS settings

! This feature is depreciated, use registration forms instead.

In order to use SMS based subscribers you need to configure these settings. You also need to

enable SMS as a payment method in the portal rule (layout -> portal page -> rules) and as login possibility in the portal (layout -> portal page).
Users can then login with their mobile number (without the + sign) and password which they received via SMS.

Please note that your portal needs to have an SMS based page, please contact support if this is not the case

There are 2 ways to send an SMS:

- via SMTP, an e-mail will be sent to the SMTP server
- via http (kannel interface)

SMS server configuration
This will set the sender, destination and subject of the e-mail.
Destination can be [mobile number] + destination (01234678@example.com) or just destination domain (test@example.com)

SMTP settings
SMTP settings to be used when sending an e-mail to the SMS server. This is most likely not configured correctly if users get an error message: cannot contact server.

Billing plan
The billing plan that will be used.

Password settings
Choose how the password needs to be made.
If renew is enabled, passwords will be renewed when the user requests his password again.
If you want to resend the password again when an account is still valid and the subscriber presses "request", you need to enable resend here.

Mobile settings
Determine how a valid mobile number should look like.

SMS window
Passwords can only be requested between those hours.

4.8 Devices

4.8.1 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 then use a technical representation of the device like the user agent or mac address.

4.8.2 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.

4.8.3 Use

Devices can be used to

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

4.9 Free access

! This feature has been depreciated, use registration forms instead.

4.9.1 Introduction

The free access module is a self registration tool for subscribers. When a free access configuration is enabled in the portal rules, the subscribers can register using a form and they get free access.

4.9.2 Configuration

Select the fields you want to be visible in the self registration portal, you can specify if it is a required or optional field. Select a free access billing plan, validity and recurrence can be configured the billing package (see Billing). Enter a name for the free access configuration.

In the portal rules, the free access plan will be visible in the payment section and needs to be selected there.

4.10 Groups

4.10.1 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.

4.10.2 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)

4.11 LDAP settings

4.11.1 Introduction

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

4.11.2 LDAP servers

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

4.11.3 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

4.11.4 LAN rules

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

4.12 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.

4.13 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 room 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.

4.14 Rules

4.14.1 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

4.14.2 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.

4.14.2 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.

4.15 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 specified time.

Notes 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. (Locations can be created in the home screen)

4.16 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.

4.17 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, ...

4.18 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 succesful.

- 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.fdxtended.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.fdxtended.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 sent 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")

5. Billing

5.1 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

5.2 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.

5.2.1 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.

5.2.2 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.
- Calender days: The account is only valid on the days /hours specified in this calender 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 to 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 expired, 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.
- Accounting Interim Interval: interval on which the profile is updated with the latest data / time usage.
- 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.

5.3 Calendar days

Calender 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.

5.4 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.

5.5 Upgrade Packages

version: 4.6.04 or up

Hospitality feature

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.

Configuration

In settings => general 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 you 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. Layout

6.1 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.
- Theme: The look and feel of the gateway.

6.2 Portal page

6.2.1 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.

6.2.2 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: (depreciated) you can only change the colors and text.

6.2.3 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).
- SMS, with this users can login using their mobile number and an access code they received via SMS. This option can only be used if SMS is also enabled as payment method in the portal rule. If SMS is enabled as payment method but SMS is not enabled as login method, guests will be able to login with just their access code received via SMS.

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.

6.3 Portal editor

6.3.1. Introduction

The portal editor is a tool provided by the HSMX gateway to create portal pages, all modules provided by the HSMX firmware are supported by the portal editor (free access, voucher, in house guest, view bill, …). This portal editor makes sure that HTML and PHP knowledge is no longer needed to create a custom portal page. The portal editor will create all the HTML and PHP code for you depending on the options you select.

6.3.2. How to start

The steps to create a portal page with the editor are almost identical to any other portal type. Go to the layout -> portal page, press the “add portal page” button and make sure you choose “HSMX portal” as portal type. An additional section will appear when you edit the portal: “Edit portal, Go to editor”. With this button you will be able to view the editor, all changes based on the layout will happen in this editor.

6.3.3 Portal editor menu

Two menus can be found in the portal editor, we have the main menu (fig. 1) on top and the quick menu (fig. 2) that will appear when selecting a container in the editor. All menus found on the quick menu are also present on the main menu.

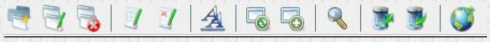


Fig. 1

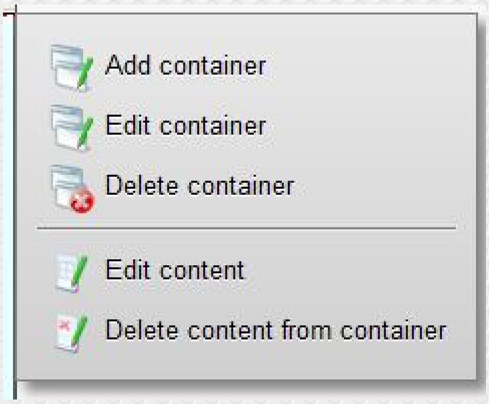


Fig. 2

We will go over the main menu from left to right:

- Add container: This option will add a container inside the selected container, there is no limitation on the amount of containers you want to add.

- Edit container: Change the layout of the selected container, all changes will apply on all containers sharing the same layout. This can happen if you choose the option "clone" when creating a new page.

- Delete container: Delete the selected container, the container will be removed. This will not delete content that is part of this container, all content can be simply reused later on.

- Edit content: Add / edit / remove content. There are 2 kinds of content: user created and predefined forms. Forms are used to interact with the HSMX (display billing plans, login, subscribe, …).

There are a few scenarios supported by this option:

1. If a container is selected and has content: You can edit the content that is already visible in the container. The content will also change in other containers if the content has been reused.
2. If a container is selected and has no content: You will get the option to create new content, reuse existing content or clone an existing content. The content will automatically be linked to the container. Options are:

a. Create: this content will only apply on the selected container.

b. Reuse: the content will be reused, all changes will reflect on containers sharing the content.
c. Clone: Create a new content but use a specific content as template.
3. No container is selected: See point 2, the only 2 differences are that the content will not be added to a container and that the option "Remove" will be available. This way you can delete content that is no longer needed.

- Delete content from container: This will delete the content from the selected container. This does not remove the content from the database.

- Edit link style: Create, edit or remove link styles. Link styles can be used to give your hyperlinks a specific layout (useful for creating a menu). Hyperlinks can be added when creating or editing user created content. When creating a hyperlink in the "edit content" menu you will be able to choose the class you created in this menu (edit link style). All styles applied to these hyperlinks are not visible in the editor.

- Change page: Here you can change the current page. Page names in read are pages that are already created. Clicking on a page will either show you the already created page or give you an option menu where you can choose to create a new page or clone an existing page.

All pages are displayed in groups. This does not mean that you have multiple pages (there is only 1 index page although you will see this page several times). These groups help you to determine what pages can be used in a specific flow.

- Add page: Add your own custom page. This page will become available in the "change page" menu. Linking from one page to another can be done by hyperlinks.

- Find container: When you are unable to select a specific container (too small, inner container is blocking access, lost, ...) you can click this button. This button will add a space to every container so it becomes a bit larger making it possible to select.

- Publish: This will make the portal available on your gateway. You need to publish your portal page once you are done editing. If you make a small change afterwards you have to publish the portal page again.

- Export: Export the complete portal.

- Import: Import an exported portal. Only portals created by the portal editor can be imported.

4. Containers
Containers are the building blocks of a portal page. Containers are used to create your layout and it is here you place content, images, forms,… All pages will start with 1 predefined container, this container will be used as your main background (body) when you open the portal in a browser.

To remove an entire page you can simply delete the main container.

All styles added to a predefined form (content) will be stored in the container having this form. This means that if this container is being used on a different page and having a form of its own, you will overwrite the form specifications by the new form options. Therefore it is best to create a new container before adding a form, this way you are sure the layout is stored in a unique container.

5. Container options

- Parent: The container having the container we are speaking of.
- Child: The container inside the container we are speaking of.
- Dimensions

o Width: the width that will be given, this can be in pixels, auto or in percentages, percentages will be calculated based on the width of the parent container. Auto will look at the child elements.

o Height: the height that will be given, the same options as width are present.

- Container position

o Stretch: The container will use the entire width, meaning the next container inside the same parent will be placed beneath this one.

o Middle: The container will be placed in the middle of the parent container. The next container inside the same parent will be placed under this one.

o Left: The container will be placed on the left side. If another container will be placed in the same parent container having the value left or right and there is still enough room in the parent container then this container will be placed next to the other one.

o Right: The container will be placed on the right side of the parent container. Apart from this the same conditions as left are being applied.

- Padding: Padding will create an empty space outside of the container but the border will be applied after the padding value. Meaning if you have a container of 20 pixels width and padding 5 pixels, the border will be showed at 25 pixels.
- Margin: Margin will create an empty space outside of the container but the border will be applied before the margin value. Meaning if you have a container of 20 pixels and margin of 5 pixels, the border will be showed at 20 pixels.
- Border: The border that will be showed, if you have problems removing a border (if a browser applies one automatically), you can choose a border type (like solid) and just pick 0px as width.
- Background

o Color: background color, if no color is selected, the container will be transparent.

o Image: Image that should be showed on the background.

o Image repeat: If the image should be repeated or not.

o Image position: The position of the image inside the container.

- Border radius: This option gives you the ability to create rounded borders.

- Border shadow

o X-position: the horizontal start position of the shadow.

o Y- position: the vertical start position of the shadow.

o Blur distance: The blur distance.

o Spread distance: how fare the shadow should reach.

- Overflow: This option will determine what should happen with context / child containers having a larger area than the selected container.

o Visible: The inner content will go over the parent container.

o Auto: Scrolls will become available if needed.

o Hidden: All content not matching the parent container will become invisible.

o Scroll: Scrolls will be visible no matter what.

6. Limitations

The HSMX provides the tools to create your own portal page without the need to know anything about HTML and PHP. The HSMX will create the HTML code based on the actions you have taken but cannot guarantee the actual outcome of the page. All depends on what browser you are using and if the browser supports the options provided by the HSMX. The portal editor uses the latest standards in HTML and CSS therefore we recommend to always use the latest version available for your browser.

6.4 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).

6.5 Logout page

Description

The logout page is a page where the client will be redirected to after they logout.

Use

Upload a ZIP archive that contains"index.html"

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	

7. Extra

7.1 Introduction

The extra menu is mainly collection of reports.

- Real time bandwidth report

- usage reports

- logging

....

7.2 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.

7.3 Reports

7.3.1 Introduction

The reports module gathers all kind of statistical data from the user database.

7.3.2 Graphical reports

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

7.3.3 Sessions

Here you need enter a number of different criteria, and then click generate report (there is also an option to search using all field, or just one field). This will bring up an excel sheet that displays all the subscribers and session information. You can save or print the file from here if necessary.

7.3.4 Revenue export

This will bring up an excel file, displaying the revenue for a certain period.   You can save or print the file if necessary. Select the time period that you wish the view.

7.3.5 Subscriber export

In this section you can generate a report for all users who were created between specific dates.

7.4 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)

7.5 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

7.6 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.

7.7 Currencies

Here you can update and add currencies to be used for billing purposes.

7.8 Password policy

In the password policy you can set different password policies for the system. Password policies are used on the portal page and define actions the guest has to do concerning his password. Also an administrator account can be tied to a password policy.

- 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.

7.9 Portal debug

Portal debug is an advanced debugging feature of the portal page sessions.
You can enable portal debug in system => system settings. (see system settings).
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.

7.10 Summary

The summary is an overview of the major settings of the HSMX.

It is possible to generate a PDF by clikcing the top right button.

8. Network

Here you will find the most import (WAN) network related settings.

- Network configuration

- Firewall

- Cluster

- Network policies

-...

8.2 Cluster

version: 4.6.04 or up

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.

8.3 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 / ...)

8.4 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.

8.5 Custom DNS

You can configure the system to resolve certain domains to an ip address rather then to forward the request to the DNS server. It is also possible to forward the DNS request for certain domain names to a separate DNS server (enabled forward instead of resolve).

Tip If you want to respond to all DNS queries, eg when there is no WAN connection, use # as domain name and forward to any IP address not used by the system.

8.6 Firewall

8.6.1 Introduction

The firewall modules 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.

8.6.1 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

8.6 Load balancing

Load balancing will automatically spread the load of all subscriber sessions over the different WAN interface are 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 that will be assigned to that WAN interface. The option failover allows that an interface can be used when another WAN interface is down.

8.8 Network configuration

8.8.1 network configuration

In this module you can configure the ip settings for each network port or VLAN in the system. Click on add to add a new IP configuration, there you can choose between static, DHCP and PPPoE.
Static
In this mode, you need to enter a name, IP address, netmask, network port and optionally the default gateway.
DHCP
Here you only need to enter a name and network port.
PPPoE
You can choose this option if you want to connect to a DSL device. Just enter a name, username, password and network port.
In the advanced settings you can configure the speed, duplex, autonegotiation and MTU settings of an interface.

Default WAN interface: This is the interface where the default route will be set to.

Monitor

Enable monitoring for the interfaces you want to see reports. The interface will be checked each time and will influence the health status of the machine.

Current IP configuration:

The current configuration applied to the system, use this to verify your changes were successful.

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 bridget 2 or more (virtual) interfaces.

The (virtual) interfaces can be used to assign a network configuration (see above 8.8.1) or they can be used as listen port for the LAN (subscriber networks).

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 DNS

Enter up to 3 DNS servers the system can use to forward the DNS requests to. You can use the Connection test utility to verify if the gateway can resolve domains.

8.8.5 DynDNS

When you have a subscription with DynDNS or no-ip and have a dynamic WAN ip address, then enter the details of the service to use DynDNS or NO-IP to get access to your device even if the public IP changed.

8.8.6 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.

8.9 Network policies

Network policies is in fact a client firewall.

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.

Example1, it is possible to rate limit and redirect SMTP traffic to your own SMTP server so clients that have a SMTP server configured that does not allow relaying can still send e-mails because the redirect makes sure your mail server handles the request.

Example2, it is possible to forward the http traffic to a proxy server of your ISP.

A network policy needs to be activated either in the billing package or in the subscriber plan (see global settings)

8.10 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.

8.11 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.

8.12 port forwarding

8.12.1 Introduction

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

8.12.2 Requirements

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

Best practice is to add the device MAC address and IP address in the static DHCP options of the subscriber network. The MAC address needs to be added to the user database. The gateway needs to be configured with a static WAN IP address.

8.12.3 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.

8.13 QoS

8.13.1 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.

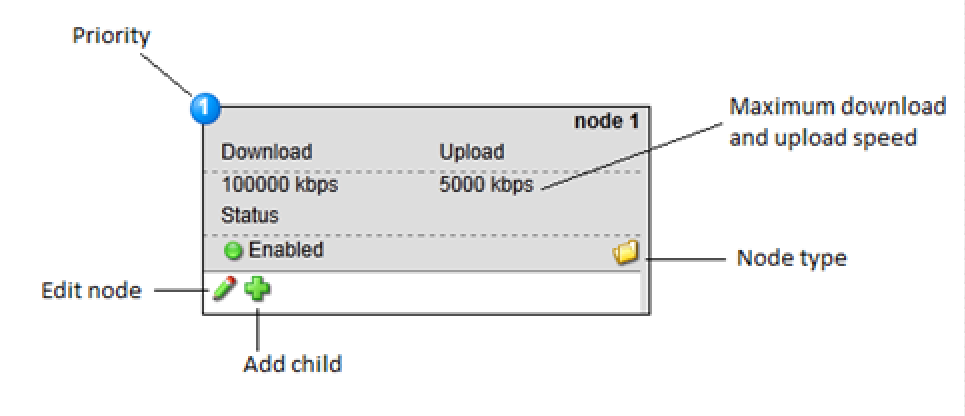
8.13.2 Interface

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.

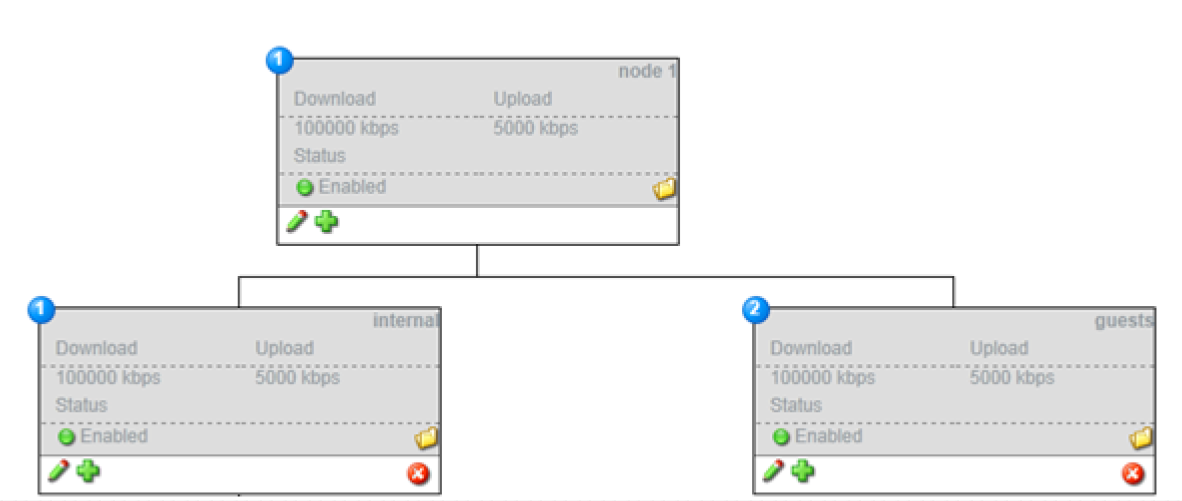
If a node shows a funnel icon then this node has a network policy, network policies can be used to divide the bandwidth of a node by using rules.



8.13.3 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:



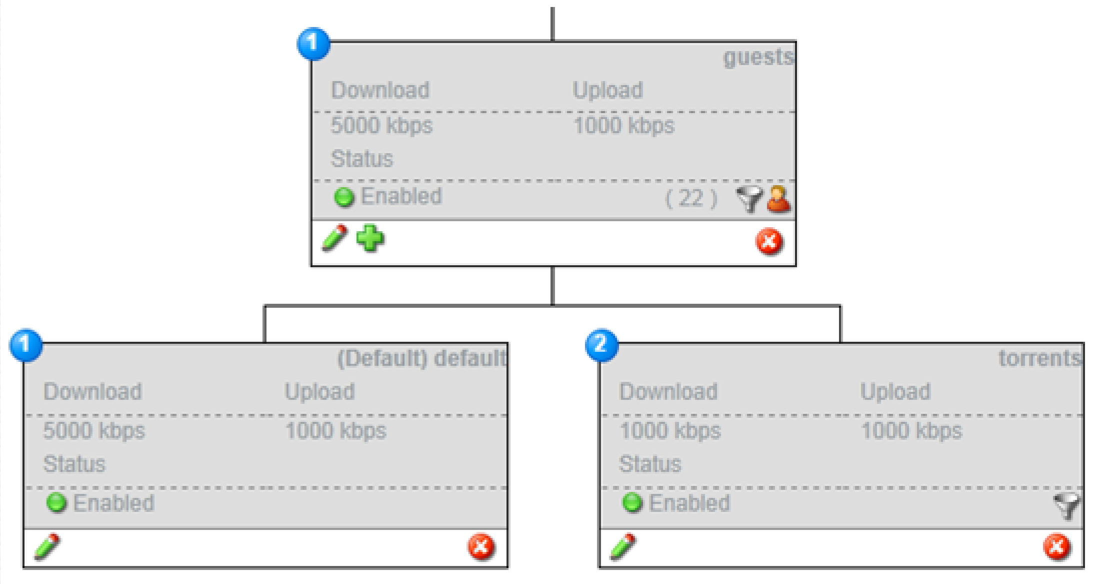
Clients in node Internal will have higher priority as clients in node guests. This means that bandwidth will go from the guests node to internal node if needed. As soon as the internal node doesn't need the bandwidth anymore, the guest node will have his full capacity back.
The total download bandwidth 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:



1 guests

Download	Upload
5000 kbps	1000 kbps
Status	
Enabled	(22)

1 (Default) default

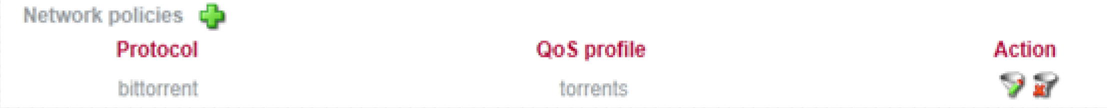
Download	Upload
5000 kbps	1000 kbps
Status	
Enabled	

2 torrents

Download	Upload
1000 kbps	1000 kbps
Status	
Enabled	

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:



Network policies

Protocol	QoS profile	Action
bittorrent	torrents	

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).

8.13.1 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.

9. LAN (subscriber network)

9.1 Introduction

A subscriber network is a LAN network segment that operates with its own settings. Configuration of a subscriber network contains:

- network setting

  LAN subnet

  DHCP server

  DNS settings for login domain

  LAN port (or VLAN)

- logical settings

  walled garden (free sites)

  Default bandwidth

  Default QoS profile

  Default network policy

- Authentication settings

  local authentication / external RADIUS / realm based roaming

  Internal portal / external portal

The HSMX is not limited to a single LAN network, it is possible to create several networks. There is a good reason to create a few subscriber networks:

- Spread the load of your network over multiple subscriber networks

- If you have 2 separated networks that are independent and have individual settings.

9.2 Add subscriber network

To add a subscriber network, click on LAN => Add subscriber network. This will start a wizard that will guide you through all different settings.

9.3 LAN global settings

In the global settings menu you can enable or disable the subscriber network and choose between layer 2 and layer 3. When using layer 3 you need to add all subnets (network settings -> subnets tab, see 3.4.4.3) that will be used in the L3 network.

In Location name you can change the name of the subscriber network. Since you can configure a subscriber network per VLAN or per physical network port the name should clearly identify the exact location.

The option virtual subscriber network turns makes the subscriber network virtual and authentication will happen on a centralized gateway. (See LAN client / server model)

You can also set a content filter or network policy on each subscriber network. When a client connects to a subscriber network that uses a content filter/network policy with a billing plan that also uses a content filter/network policy then the billing plan settings will be used instead of the subscriber network settings.

9.4 LAN Default settings

In the default settings menu you can change the values by default for:
idle time-out:

The amount of time that the subscriber must remain idle before automatically being logged of

bandwidth up:
Available bandwidth for uploading in Kbytes/s
bandwidth down:
Available bandwidth for downloading in Kbytes/s
Note Default settings will only be used when AAA is disabled.

9.5 LAN advanced settings

The LAN advanced settings should only be changed when instructed by support. A short description of the configurable modules:

- State file: The state file is used to restore the user sessions when the subscriber network is restarted for configuration change or system reboot.

- Debug mode: Enabled debug logging of the subscriber network daemon. be careful this will consume resources and could fill up storage space in matter of days.

- VLAN update: could be disabled to free some resources, when a client roams from one vlan to another, this script will verify what needs to happen with the authentication state of the user (stay connected / re login / free access, ...)

- MAC up: Script that checks the authentication status of all new devices that access the network (rather then wait for a portal redirect)

- Advanced interface settings, set fixed speed / disabled auto negotiation / MTU size. Only change this when there are problems with the auto negotiation with the switch.

- ARP spoofing is a tool to improve roaming across multiple subscriber networks, this updates the RAP cache of all clients on interval so if the ARP cache is wrong, it will be updated in a few seconds. You need to enter all LAN ip's and optionally vlans's if there are multiple VLANS per subscriber network.

9.6 LAN network settings

9.6.1 network interfaces

Here you specify the LAN Interface and WAN interface for this subscriber network. Only the default WAN interface is available unless load balancing is enabled (Network -> Load balancing). It is possible to specify a WAN alias ip to get more NAT connections if you have multiple subscriber networks and WAN IP's.

VLAN support
If you are making use of VLAN tags in your network you can enable VLAN support for this subscriber network. If this is enabled you can attach rooms/locations to a specific VLAN.

Do not enable VLAN support if your LAN port is already a VLAN port.

VLAN roaming

This option can only be enabled if listen to all VLAN's is enabled.

Traffic forwarding

By default traffic forwarding to interfaces other than the WAN interface(s) is blocked. Unless you specify another network port here.

9.6.2 network settings

In the network settings tab you can confirm the global network, DHCP and Any IP settings.

Global Settings
Here you specify the IP pool to be used for your clients. You just have to fill in the LAN IP and LAN subnet and the system will automatically generate the pool that can be used. Any IP setting is only important to support clients with a static IP address (even when they are not in this range).

DHCP Settings
Disable: no DHCP server
DHCP server: the HSMX will give out IP's from this pool to the clients.
DHCP relay: if you want to use another DHCP server, you need to enter the gateway IP and port of the DHCP server and the public WAN IP from this appliance in order to use this option.

You can enable DHCP broadcast to broadcast all DHCP replies, only use when needed.

Any IP Settings
This setting allows subscribers with a different IP than the DHCP pool.
You can use the advanced any IP settings to ignore a specific IP or subnet.

Logout IP
This IP address can be used to logout as a client.

9.6.3 subnets

You can configure more subnets, and specify if the gateway needs to NAT connections originating from this subnet (private pool).

The subnets tab is mainly used in layer3 mode, then you need to specify all subnets so the gateway knows how to deal with the client connections / DHCP requests. In layer2 mode it is also possible to add a public subnet, clients who have an ip from this subnet will then be excluded from natting.

9.6.4 static DHCP

This module will force the dhcp server to reserve the configured IP for the configured MAC address.

9.6.5 DNS settings

Here you can configure the domains that can be used from the subscriber side.

Domain
Domain that will be used during the DHCP assignment.

Login domain
This domain is the logical name that users will see in the URL of their browser when they are redirected to the portal page.

Logout domain
This domain can be used to logout

Status domain
The status domain can be used to open a status page with the status of the client connection (needs to be enabled in the portal).

Upgrade domain
To upgrade an existing account, the subscriber can only use this domain if the subscriber is active, the subscriber has bought an account with PMS and if the portal has an upgrade page.

9.6.6 VLAN definitions

A list of all VLAN's in this subscriber network. You can export / import VLAN's by pressing the import / export button or you can add a VLAN by pressing the add button.
In the action column you can edit or delete a VLAN. When creating or changing a VLAN you can attach the VLAN to a location or room. You can also choose the AAA state this VLAN.

9.7 LAN AAA settings

9.7.1 UAM

In the UAM (Universal Access Method) server screen you can enable or disable:

AAA
By enabling AAA you make sure subscribers will be redirected to the login page and have to log in before accessing the Internet

Pre authentication URL
You can make use of a pre authentication URL before users get to the portal page. To do this just enable pre authentication URL and fill in a valid URL. It’s important that the GET variable “redirect” is set when the user is redirected back to the portal. Without this variable the client will always be redirected to the pre authentication URL.

SSL
Only enable this option if you have SSL enabled on the appliance and make sure the SSL certificate is registered for the domain you’ve configured in the DNS settings of the subscriber network. This way the users will be redirected to a SSL protected login page without being warned about an invalid certificate. By default the gateway ships with a valid SSL certificate for login.fdxtended.com.

Https

The server will also repsond to https requests for non active devices. An SSL warning will always be given by browsers as the domain will not match the SSL certificate of the gateway.

Server Type
Use server type external to redirect the users to an external server instead of the internal server portal.

9.7.2 RADIUS

Here you can choose between 3 different options

- Internal: Use the internal authentication database of the gateway
- External: Use an external RADIUS server
- Realm based: Use a pattern to determine which RADIUS server should be used. (Wildcard * can be used)

RADIUS profiles can be added in Settings - RADIUS profiles.

9.7.3 Walled garden

IP addresses / domains or URLs in this list will be accessible for all subscribers in this subscriber network without authentication. Below you can see all different configuration options for the walled garden. In case a walled garden entry could not be activated it will turn up with a red icon, when you hover your mouse over the red icon you will see the reason it was rejected. There is an import and export utility so your walled garden list can be easily transferred to other gateways or subscriber networks. The disallow feature is only for use with regular expressions. When disallow is enabled, the system will deactivate it when it is set on standard walled garden entrees (not regex) when the configuration is applied.
Examples

Ip addresses
Standard: 1.2.3.4
With subnet: 1.2.3.0/24 (allow entire subnet)
With port: 1.2.3.4:443 (only allow access to port 443 (https) on this host)
With subnet and port: 1.2.3.0/24:443 (allow https to every host on this subnet)
With protocol: icmp:1.2.3.4 (allow ICMp to this host (ICMP => ping)
With protocol and port: tcp:1.2.3.4:443 (only allow TCP connections to port 443 on this host)
With protocol and subnet: icmp:1.2.3.0/24 (allow ICMP (ping) to every host is this subnet)
With protocol, subnet and port: tcp:1.2.3.0/24:443
Tip To allow access to every ip on the Internet (e.g. https) you can use: 0.0.0.0/0:443

Domains
Standard: www.host.com
With port: www.host.com:443 (allow https to www.host.com)
With protocol: icmp:www.host.com
With protocol and port: tcp:www.host.com:443
With wildcard: *.host.com (allows all subdomains of host.com)

Regular expressions
www.host.com, allow: www.host.com is allowed
www.host.com/^maps, disallow: everything of host.com is allowed except where the path starts with maps
host.com/^(maps|books), allow: allows every URL of host.com where the path starts with maps or books
^host.com/* (allows host.com but not www.host.com)

Note The regular expression check can put a lot of load on the system if there are a lot of pending users. This check also doesn't work on https connections.

Note2 The regular expressions supports only one entry per host, having multiple items that match the regular expressions can give unpredicted results.

9.7.3 Black list

This module can be used to block a domain for all users in this subscriber network.

9.7.4 MAC based authentication

This module will do a RADIUS authentication request to the configured RADIUS server as soon as a new device is detected on the network. If the radius server accepts the request, the device can connect without any other further authentication.

9.8 LAN subscribers

In this menu you can find an overview of the current subscribers in the selected subscriber network. The overview shows the following parameters:

- *MAC* Layer 2 only

The MAC address of the subscriber. By clicking the MAC address you can see an overview of the subscriber. In this overview you can release the MAC address, add it to the database or remove it from the database

- *IP*

The IP-address of the subscriber

- *AAA State*

Shows if the subscriber is logged into the network (VALID) or attached to the network but not logged on (PENDING)

- *Username*

The username of the subscriber

- *Active*

Shows how long the subscribers has been active on the network

- *Timeout*

Shows how much time the subscriber has left on his account

- *Idle timeout*

Shows how much time is left before idle time-out

- *Input*

Shows the amount of data that has been downloaded by the subscriber

- *Output*

Shows the amount of data that has been uploaded by the subscriber

- *Band.Up*

The limitation on the bandwidth for upload

- *Band.Down*

The limitation on the bandwidth for upload

- *First URL*

The first URL that was visited by the subscriber

- *VLAN*

Which VLAN the user is connected to.

It is also possible to click on the MAC address of a subscriber to see all the details or to add the MAC address to the internal database so this MAC address no longer needs authentication.

Note You can release all DHCP leases by clicking on the top right image.

9.9 LAN Client / Server model (virtual subscriber network)

version: 4.6.04 or up

Introduction

The HSMX client / server model separates the portal / authentication server from the physical network gateway. This can be used for several reasons:

- To centralize several small locations and allow roaming between these locations.

- To separate the services over multiple devices to achieve a higher performance in very large networks.

Operation

The client HSMX will open an authentication tunnel to the central HSMX that stays up all the time, the tunnel is used to sync the information from client to server and from server to client. With this approach, the client HSMX doesn't need to have a static public IP address since the client always initiates the tunnel to the authentication server. The authentication server will serve the portal to the clients and will therefore handle all billing and authentication.

Configuration

Authentication HSMX

The authentication server listens on TCP port 5001 for connections from the client HSMX gateway. This port must be enabled in the firewall.

Configure the firewall via Network => firewall configuration.

!For safety reasons it is best to include the source IP / sub-net of the client HSMX in the rules so the service cannot be exploited by other systems.

Client HSMX

On the client HSMX, there is an option per subscriber (LAN) network to enable "virtual subscriber network". This option can be found in "LAN => global settings". When the option is enabled, a new tab will show up called "virtual subscriber network settings". In this tab it is possible to configure the IP of the authentication HSMX. In the breadcrumb you can see if the connection of the authentication tunnel is up. When it is up, it is possible to start the authentication process of the clients and to sync the configuration from the client HSMX to the authentication HSMX.

Limitations

The client server setup by design makes the following modules unavailable:

- QoS

- Content Filtering

- Network Policies

- WAN load-balancing

Troubleshooting

Connection to the authentication HSMX cannot be established

Make sure that the authentication HSMX allows TCP port 5001 for the ip of the client HSMX. The connection to the authentication HSMX can be tested via Network => connection test, enter the IP of the authentication hsmx, port 5001 and a timeout of 5 seconds.

The authentication HSMX doesn't show the subscriber network of the client HSMX

The configuration can only be synced when the authentication tunnel is up, so first make sure the connection is up, the global health status of the client HSMX show whether there is a problem or not.

When the tunnel is up, reload the configuration of the subscriber network to trigger it to sync to the authentication HSMX.

No portal page is displayed

If the connection to the authentication HSMX is different than the WAN interface, make sure you enable forwarding to the required port in "LAN => network settings".

Make sure the authentication server accepts http(s) connection from the IP of the client HSMX, this can be tested via "Network => connection test".

Check out the FAQ in case the above did not solve the problem.

10 System settings

10.1 Introduction

The system menu lists a variaty of modules to manage the system. This includes:

- access control

- backup / restore

- filtering

- reboot

- ....

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 settings - 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 te 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 Content filter

10.3.1 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.

10.3.2 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".

ImportantYou 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.

10.4 FTP based configuration

This module is for emulation of older software that retrieves some configuration over the FTP module.

10.5 Factory reset

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

10.6 Filters

Portal filters

Filters are designed to answer to specific User agents, hosts and paths 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.

10.7 Intrusion detection

10.7.1 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.

10.8 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.

10.9 System 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.

10.10 System Performance

version: 4.6.04 or up

10.10.1 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.

10.10.2 Configuration

System => Performance

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 * the amount of public ip's. At least when these public ip's are used for natting.

10.11 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.

10.12 System SSL

With this module you can manage the SSL certificate of the webserver.

Standard the system is loaded with the certificate login.fdxtended.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.

10.13 System backup

10.13.1 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.

10.13.2 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.

10.13.2 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.

10.14 System settings

Subscriber session timeout
When a subscriber is idle, the system needs to calculate the session time the profile has left. Here you can choose the difference between start and stop time or the session time provided by the gateway. This can be different, as the session time of the gateway usually does not include the time the user has been idle.

Clear database
To clear the database there are two settings:

Expired users will be moved to the archived subscriber list
Idle users will be moved to the expired subscriber list

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 arround.

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 retuned 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.

Portal debug

Here you can enable the portal debug feature to debug the portal sessions.

Depreciated mode
Some featues have been replaced by other functionalities. You can hide all depreciated features by disabling this feature.
Features that have been replaced are:
- Billing -> free acccess, 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.

10.15 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.

10.16 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 taks manager also gives a clear picture of memory and CPU usage of the system. In case you get a blanc page, increase the refresh rate.

10.17 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.

10.18 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.

10.19 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.