



CO.IN.

Content Injector

Web Cache

Antivirus

Blacklist

Administrator Manual
Manual Version 1.0.0

March 2017

PROMETEO S.R.L.
Via Roma, 61
31010 Fonte
Treviso
Italy
Tel. +39 0423 9292
Fax. +39 0423 929392
info@hsnetworkmanager.com
www.hsnetworkmanager.com

THE SPECIFICATIONS AND INFORMATION CONTAINED IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT ANY NOTICE. ALL STATEMENTS, INFORMATION AND RECOMMENDATIONS IN THIS MANUAL ARE INTENDED TO BE ACCURATE, BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED. USERS ASSUME FULL RESPONSIBILITY FOR THE USE.

IN NO EVENT SHALL PROMETEO S.R.L. OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL OR INCIDENTAL DAMAGES, INCLUDING WITHOUT LIMITATION LOSS OF PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THE MANUAL THOUGH PROMETEO S.R.L. OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Prometeo, HSNM, HsNetworkManager and logos Prometeo, HSNM and HsNetworkManager are trademarks of PROMETEO S.R.L. The third party trademarks are the property of their respective owners.

All rights reserved.

CONTENTS

INTRODUCTION 1

 STYLES 1

 GLOSSARY 2

PRODUCT OVERVIEW 3

 WHAT IS CO.IN..... 3

Who this product is aimed at. 4

Hardware Features..... 5

 COMPATIBILITY 6

 HOW IT WORKS..... 6

Introduction..... 6

Injection..... 6

Cache..... 6

Antivirus..... 6

Blacklist 6

INSTALLING CO.IN. 7

 PACKAGE CONTENTS..... 7

 CONNECTING INTO THE ELECTRICAL OUTLET 7

 TURNING ON 7

 CONNECTING TO THE COMPUTER FOR THE FIRST CONFIGURATION 7

ADMINISTRATION INTERFACE..... 8

 SYSTEM ACCESS 8

 ADMIN LAYOUT 9

 SYSTEM TOOLBAR 10

System Information 10

 Company..... 10

 General Information 10

 Uptime 10

 Service Status..... 10

 CPU 11

 Network 11

 Ping 11

 RAM 11

 Hard Disk..... 11

Utility Functions 12

 Sending a Test Email 12

Close Session 13

 Disconnecting User 13

 Rebooting the System..... 13

 Shutting Down the Appliance 13

 THE SIDEBAR 14

"Admin" Tab 14

 THE DATA AREA 15

Commands..... 15

Nav Buttons..... 15

 MANAGING CONTENTS 16

Dashboard..... 17

 Tile Types of the Dashboards..... 17

Tables 21

Pages for Inserting or Editing 22

Context Menu..... 22










FIRST LOGIN TO THE ADMINISTRATION INTERFACE..... 23

 ASSIGNING NETWORK PARAMETERS 23

 CONNECTING TO YOUR NETWORK 24

 UPDATING THE SOFTWARE 25


ADMINISTERING THE SYSTEM..... 26

- INTRODUCTION 26
 -  **General Options** 26
 - General Info 26
 - Logos for System Administration 26
 - System Settings** 27
 - License 27
 - Network 27
 - Web Server 28
 - Data Optimization 29
 - Email Messages 29
 - NTP 30
 -  **INJECTOR** 31
 - Options 31
 - HSNM 31
 -  **STATIC ROUTES** 32
 - Data 32
 -  **PROXY & CACHE** 33
 - Options 33
 - Bypass Proxy 34
 -  **BINDING IPs TO NAMES** 35
 - Data 35
 -  **ANTIVIRUS** 35
 - Options 35
 -  **BLACKLIST** 36
 - Options 36
 -  **DOCUMENTATION** 37
 -  **UPDATES** 38
- ACTIVATING CO.IN. IN HSNM** 39
- REMOTE ASSISTANCE REQUEST** 40
- PORTS TO OPEN ON YOUR ROUTER/FIREWALL** 40

Introduction


Styles

This manual uses styles, fonts and symbols specific to the context in order to facilitate the reading and then create a symbolic association with the capabilities of the product. The icons used are those present on the pages and in the context menu of the configuration.

 Means *pay attention and take note of the helpful suggestions*. In some places, in order to study or to highlight some important aspects, notes have this side note icon and this background.

Glossary

The table below shows on the left the abbreviations used in this manual and on the right their meaning.

Term	Meaning
CA	Certification authority. Authority that issues the certificates for SSL connections.
Cache	It is a system that allows you to store contents in a local memory to supply them directly to later requests without contacting the server again. It also reduces the used internet bandwidth significantly, improving performances and user experiences.
CO.IN.	Content Injector.  In order to use CO.IN. as a content injector, you must have a HSNM with the Welcome Portal & Advertising Module licenses.
CSR	Certificate Signing Request. File generated by CO.IN. to be sent to the CA to obtain a valid certificate for SSL connections.
CTR	Click through rate. It is the percentage derived from the ratio of the number of clicks and the number of views (impressions) of an advertising campaign.
DMZ	Demilitarized zone. It is an isolated LAN segment (a "subnet") accessible from both internal and external networks.
GUID	Globally Unique Identifier. Term used to: identify the license of CO.IN.; identify a product in a voucher.
HSNM	The HSNM.
NAT	Network Address Translation. It is a technique that consists in editing the IP addresses of packets in transit on a router within a communication between two or more hosts.
Proxy	It is a software that is interposed between the client and the server and it acts as a vehicle for handling requests and responses from one to the other.
Sidebar	Sidebar on the left that contains the administration tabs.
Tab	A chart control that allows the user to switch from a group of controls to another within the same area.

Product Overview


What is CO.IN.

CO.IN. is a system ready to use, easy to configure and supplied with an administration WEB interface. It has the most advanced technologies and it allows injecting advertising contents, information etc., defined in the HSNM advertising campaigns (Welcome Portal & Advertising optional modules), in the pages visited by users during their normal internet navigation.


In addition to the injection, the product can be used for other purposes:

- Cache: to reduce the internet bandwidth used by users and to improve the performances and experiences of the latter.
- Antivirus: the system analyzes HTTP contents visited by users and in case it intercepts contents considered damaging, it blocks the visualization and informs the user.
- Blacklist: selectable list of default categories containing hundreds of thousands of web sites or IP addresses that can be blocked because the contents are not considered appropriate for use of the service provided.

Thanks to special and advanced techniques in encryption and decryption, the injection can be activated also for HTTPS. In practice, techniques like “Man in the middle” are used but “ONLY” for advertising and/or security purposes.

 Warning! To make sure that even HTTPS traffic is processed, it is necessary the users install a security certificate. Given the difficulty of installing a certificate, the use of HTTPS is not considered appropriate for applications on HotSpot services. It is recommended to activate it if the product is used on corporate networks where devices or PCs that access the internet are known and recurring.

 Warning! Activating the injection also on the HTTPS can cause problems with certain web services.

 To inject contents in the pages visited by users it is necessary to: have a HSNM with the Welcome Portal & Advertising Module; insert the injector’s GUID in the gateway configuration; enable the gateways or the domains to the injection; create advertising campaigns.

Who this product is aimed at

CO.IN. is aimed at all users who have purchased HSNM and want to insert advertising campaigns or information during the users WEB navigation, to increase the security level of their users, to prevent the use of the internet on certain categories of web sites, etc.. It is recommended even if you want to add a Cache system to save internet bandwidth and to supply contents previously visited by users directly without requesting them to the server again.

Hardware Features

Intel® Celeron® Processor N3160 (2M Cache, up to 2.24 GHz)

2GB RAM

1 hard disk 32GB SSD;

2 network cards 10/100/1000

Certifications: CE; FCC.

Compatibility

CO.IN. has been designed to work with all the IP networks without particular configurations of existing routers. The only requirement is to use it as network gateway. CO.IN. transparently intercepts the traffic both HTTP and HTTPS (if enabled) and then it processes it, routing to the network gateway.

CO.IN. must be physically installed on each network.

How it works

Introduction

After you have configured the system section (network, etc.), you have to proceed with the parametrization based on your needs by defining whether to enable Injection, Cache, etc.

Injection

If enabled, users who surf the internet on any HTTP or HTTPS site (if set), every n-definable seconds, will be displayed contents like image, video or external URL based on campaigns defined in the HSNM, even remote, and user will be forced to view these contents for a minimum time defined in seconds.

Cache

It is an automatic system that allows you to deliver already visited contents to users without access to their servers. In this way, it helps you to reduce the traffic to the internet.

Antivirus

If enabled by the appropriate option, it analyzes the content provided to users, blocking any menaces.

Blacklist

It is an automatic and default system that prevents visualization of certain websites based on chosen categories considered not appropriate for the service provided.

Installing CO.IN.

This section will guide you through the procedure to follow for installing CO.IN.

Package Contents

The following items are included in the CO.IN. package:

- 1 x Appliance CO.IN.
- 1 x 12V Power pack
- 1 x Power cable

Warning! Before use, make sure the above items are included in the package. If anything is missing or damaged, please contact your dealer.

Connecting into the Electrical Outlet

After opening the package, connect the CO.IN. into the AC power outlet using the supplied power pack.

Turning On

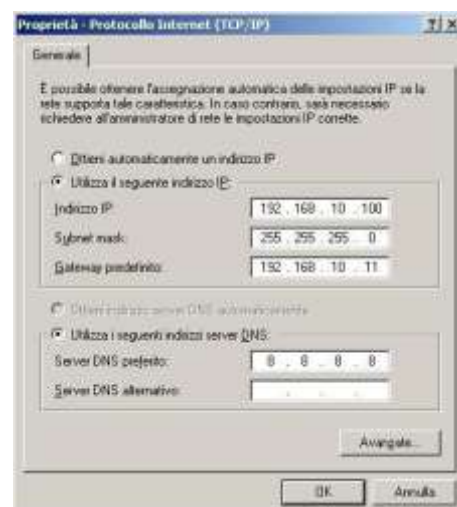
Turn on CO.IN. using the appropriate switch on the front panel of the appliance close to the “SW” word. If the button is red, it means that CO.IN. is turned off, while if it is blue it means that CO.IN. is on. Switching and start last about one minute.

Connecting to the Computer for the First Configuration

Connect the Ethernet port of CO.IN. to a computer.

Define in your PC an IP address of the 192.168.168.0/24 class (e.g. 192.168.168.100).

Warning! In the PC, do not define the IP address 192.168.168.10 because it is already assigned to the CO.IN. Ethernet.



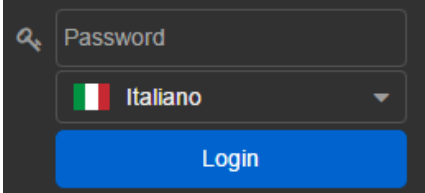
Configuration of the net in the PC

Proceed with initial configuration as described in “First Login to the Administration Interface” paragraph.

Administration Interface

System Access

By entering in the browser, the IP address or the URL assigned to CO.IN. in the "**⚙️ System Settings**" you log in a first page where you are required for password and language. After having entered the required data and clicked the "Login" button, credentials are verified and you can access to the administration of the system.

A screenshot of a login form with a dark background. It features a password input field with a magnifying glass icon and the label "Password". Below it is a language selection dropdown menu showing the Italian flag and the text "Italiano". At the bottom is a prominent blue button labeled "Login".

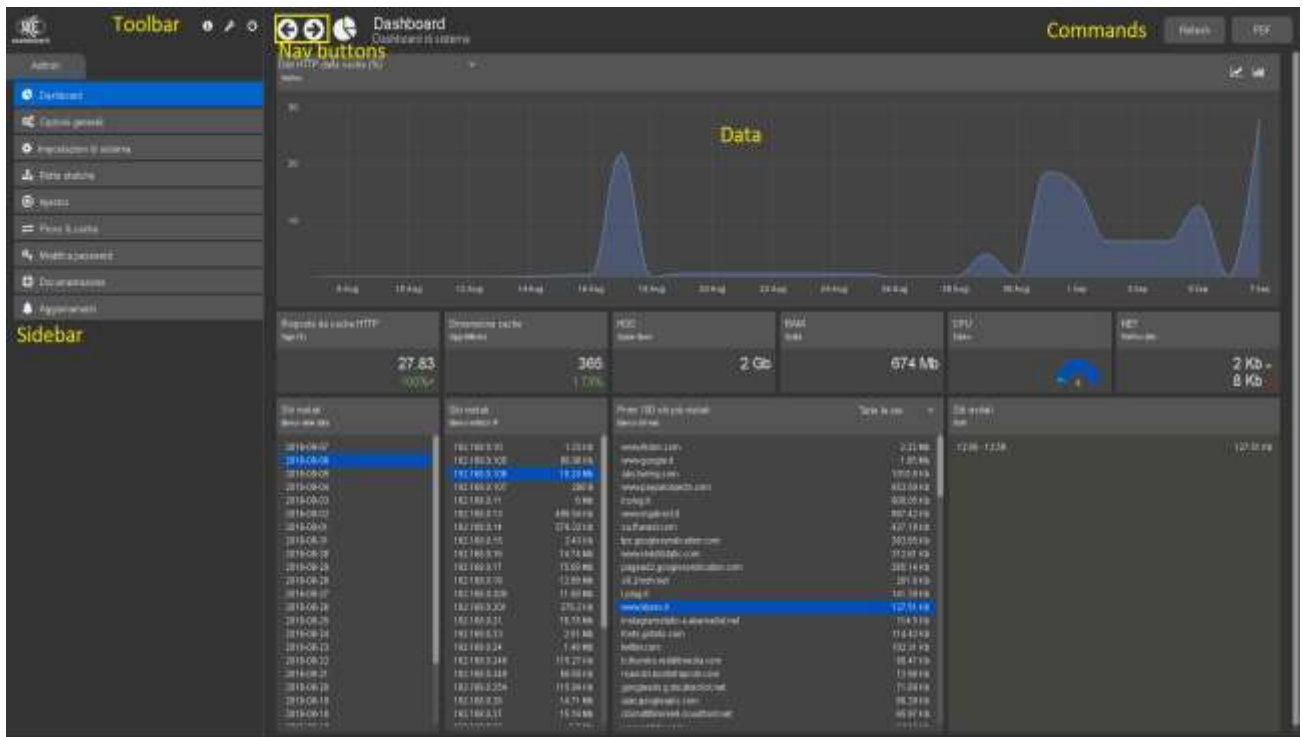
Login to the administration area

Admin Layout

The administration interface, intuitive and web-based, has been designed to simplify the management.

It consists of three main areas:

- System toolbar;
- The sidebar on the left;
- The data area on the right, which contains:
 1. Nav buttons
 2. Commands
 3. Data



View of the admin area


System Toolbar

The toolbar contains several options that allow fast access to: system information; utility functions; logout or reboot/shutdown of the appliance.

i System Information


It displays a page that contains the following data.

Company

Summary of the data of the company that is using CO.IN. and that are defined in the " General Options".

Field	Description
Company Name	Business name of the company that owns CO.IN.
Address	Address
City	City
Telephone	Phone number
Fax	Fax number
VAT-Id Number	VAT identification number.
Web Address	Website of the company that owns CO.IN.
Email	Email address.

General Information

Field	Description
System Date and Time	System date and time.
System Version	System version of the appliance. Different system features (not of hardware components) correspond to various system versions. Summary of the various versions: 10.0 on 01/09/2016: base version.
Kernel Version	Kernel version of the appliance.
Apache Version	Apache version of the appliance.
Software Version	Version of the management software and user interface. It depends on available and installed updates through "  <u>Updates</u> ".
GUID	Identifier of the appliance
Distributor	Distributor of the appliance.
Model	Appliance model and license level.

Uptime

Field	Description
Last reboot	Indicates the elapsed time since the device was last restarted.

Service Status

Field	Description
Firewall	Firewall service status.
Proxy	Proxy service status.
Scheduler	Scheduler service status.
Content Adaption	Service status for content adaption.

Antivirus	Antivirus service status.
NTP	NTP service status.

CPU

Field	Description
CPU Load Average	Reports the CPU load average, refreshed every 5 seconds.
CPU Usage Graph	Graph of CPU usage.

Network

Field	Description
Download Network Traffic	Reports the average load in Kbit (every five seconds) of the network traffic, in download.
Upload Network Traffic	Reports the average load in Kbit (every five seconds) of the network traffic, in upload.
Graph	Graph of the network traffic.

Ping

Field	Description
Host	Host to which execute the ping.
Average Ping Time	Reports the average time of the ping to the defined host refreshed every five seconds.
Graph	Graph of the ping response times.

RAM

Field	Description
Physical Memory Total	Reports the total physical memory of the system.
Physical Memory Used	Reports the used physical memory used.
Physical Memory Free	Reports the free physical memory.
Swap Memory Total	Reports the total swap system memory.
Swap Memory Used	Reports the used swap memory.
Swap Memory Free	Reports the free swap memory.



Hard Disk

Field	Description
Disk Size	Reports the size of the disk.
Free Hard Disk Space	Reports the free disk space in the data partition.
% Free Hard Disk Space	Reports the percentage of free space on hard disk.
Maximum Cache Size	Reports the maximum size of the cache of the proxy.
Cache Size	Reports the current size of the cache of the proxy.

Utility Functions

It displays a page that allows you to execute the following utility functions:

Sending a Test Email

It sends a test email to the address indicated and with the object and the text defined. Useful to check if SMTP server settings defined in the " [System Settings](#)" page, are correct and working. Any errors in sending the email will be written in the " [System Log](#)".

Field	Description
Recipient Email Address	Enter the email address to send test message.
Object	Enter the subject of the test email.
Message Text	Enter the text of the test email.

Close Session


It displays a page that allows you to access to the following options:

Disconnecting User

Field	Description
Disconnect	By clicking on the "Disconnect" button, it logs off current user's session.

Rebooting the System


By clicking the "Reboot" button after entering the correct password in the field "Admin User Password", it will run the restart of the appliance.

 The estimated time of reboot is of 110 seconds.

Field	Description
Admin User Password	For security reasons, in order to restart the appliance, you must enter the password for the Admin user.

Shutting Down the Appliance

By clicking on the "Shutdown" button, after entering the correct password in the field "Admin User Password", it will run off the appliance.

 The estimated time of shutdown is of 40 seconds.

Field	Description
Admin User Password	For security reasons, in order to switch off the appliance, you must enter the password for the Admin user. We recommend that you perform this procedure for switching off and never use the switch on the back of the appliance or disconnect power because you may lose or damage data that would compromise the operation of CO.IN.













The Sidebar

The top-left sidebar that contains the tab: Admin.

"Admin" Tab

The "Admin" tab contains a menu that allows you to configure CO.IN. at system level.

The available options are:


Option	Description
 System Dashboard	Displays the system dashboard that allows viewing statistics, graphs and data in summary format and real-time of the operating status of CO.IN.
 <u>General Options</u>	Defines the "  <u>General Options</u> " for CO.IN. such as: location; logos.
 <u>System Settings</u>	Declares the parameters of systemic configuration of CO.IN. The data processed are: license; network; web server; data optimization, mail messages, NTP.
 Static Routes	Allows you to insert static routes needed to reach the networks unreachable through the default gateway set on the "  <u>System Settings</u> " page.
 Proxy & Cache	Accesses the administration page of the proxy.
 Antivirus	Accesses the administration page of the antivirus.
 Blacklist	Accesses the administration page of the Blacklist.
 Change Password	Accesses the page to change the password to login the system
 Documentation	Provides a list of guides available for using or configuring the appliance.
 <u>Updates</u>	Accesses the system update system to enable installation of new versions.

The Data Area

This area, located on the right of the sidebar, contains the content pages that open when selecting "Admin options".



Commands

In this area, located in the top-right corner, you are displayed the command buttons that affect the current page. Examples of command buttons are "Save" to save the data, "Add" to add information, etc.

 If you edit or insert data, you will have to press the "Save" button in order changes take effect. If you change the page without saving, your changes will be lost.



In the Dashboard there is the "PDF" button that allows you to print the current Dashboard in a PDF file.

Nav Buttons

They are the buttons on the left of the title of the current page, allowing you to return to the previous  or next  page.

Managing Contents


Managing the content handled by CO.IN. is very simple and intuitive. Substantially in the system there are three types of pages that appear in the data area:

Type	Description
Dashboard	Displays information about the system performance in summary format and real-time.
Tables	The data are presented in a list and paged. If the right side of each row contains the image  , you can access the context menu that allows you to perform some context-dependent operations, such as modification, deletion, etc.
Insert or Edit Pages	Pages that contain a set of editable fields. Generally they are invoked directly from the options in the Admin tab of the sidebar, or by choosing other options like "  Edit" in the context menu.

Dashboard

Pages that, thanks to tile graphic and numeric tiles, allow you to view a summary statement about the status of CO.IN.

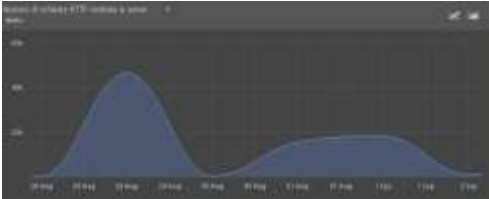



Tiles contain a title, a subtitle, a graph or textual information, numeric or tabular. The values they contain can be count, with the trend of the period selected by pressing the "Refresh" button in the command bar comparing the same number of days before the start date of the period or in real time (CPU load, network traffic; RAM used; free disk space).

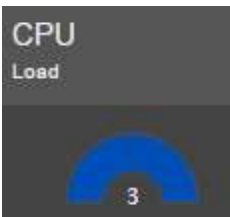

 CO.IN. uses a caching system to limit queries to the database. The values of the tiles are updated after every hour after the last query. By pressing the "Refresh" button at the top right, you force the data loading without using the cache and waiting an hour. By pressing the "Refresh" button it also recalculates the values based on the chosen period.

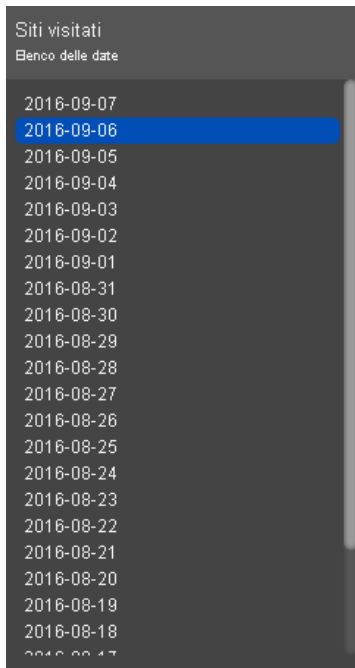
Tile Types of the Dashboards

It examines the various types of tiles that make up the dashboard.

List of types of tiles:

Appearance	Description
	<p>The main chart. It is the main chart, with lines or columns of the dashboard that contains the following data:</p> <p>Cache</p> <ul style="list-style-type: none"> • HTTP data from the cache (%); <p>Clients</p> <ul style="list-style-type: none"> • Number of HTTP requests received from clients; • HTTP data received by clients (MBytes); • HTTP data sent to clients (MBytes) <p>Servers</p> <ul style="list-style-type: none"> • Number of requests forwarded to the source server; • Number of HTTP requests forwarded to the servers; • Data received server side (MBytes); • Data sent server side (MBytes); • HTTP data received from server side (Mbytes); • HTTP data sent to server side (Mbytes); <p>System</p> <ul style="list-style-type: none"> • CPU usage in the last twenty-four hours, every minute, every 5 minutes and every thirty minutes (visible only to users who have the role of administrator); • Ethernet data rate (visible only to users who have the role of administrator). <p> The chart type can be selected by pressing the  or  buttons.</p>

<p>Risposte da cache HTTP Valori periodo (%)</p> <p>2.72 100%+</p>	<p>Responses from HTTP cache. Reports the currently cache size.</p>
<p>Cache size Current (Mb)</p> <p>19.25</p>	<p>HTTP cache size. Reports the current size of the cache</p>
<p>HDD Free space</p> <p>17 Gb</p>	<p>HDD. Free hard disk space. Real-time value.</p>
<p>RAM Used</p> <p>378 Mb</p>	<p>RAM. RAM used. Real-time value.</p>
<p>CPU Load</p> 	<p>CPU. CPU load average. Real-time value.</p>
<p>NET Bandwidth (bit)</p> <p>0 Kb ▲ 0 Kb ▼</p>	<p>NET. Total network traffic in upload and download. Real-time value.</p> <p> In the reseller dashboard, it represents the total traffic of the network interface card and not specific.</p>



Visited sites: list of dates.

It lists the dates that contain statistics on the sites visited by users. By selecting a date, it reloads the tile with the list of the IP addresses highlighting on the right the generated traffic.

The value of the generated traffic assumes the following colors:

- White: if traffic is less than twenty five MB;
- Brown: if traffic is more than twenty five MB and less than one hundred MB;
- Red: if traffic is higher than one hundred MB.

Siti visitati
Elenco indirizzi IP

192.168.0.10	1.33 Kb
192.168.0.105	80.98 Kb
192.168.0.106	10.29 Mb
192.168.0.107	286 B
192.168.0.11	6 Mb
192.168.0.13	495.54 Kb
192.168.0.14	579.32 Kb
192.168.0.15	2.43 Kb
192.168.0.16	14.74 Mb
192.168.0.17	75.08 Mb
192.168.0.18	12.86 Mb
192.168.0.200	11.08 Mb
192.168.0.201	376.2 Kb
192.168.0.21	76.78 Mb
192.168.0.23	2.51 Mb
192.168.0.24	1.48 Mb
192.168.0.248	115.27 Kb
192.168.0.249	60.65 Kb
192.168.0.254	115.94 Kb
192.168.0.26	14.71 Mb
192.168.0.27	15.19 Mb
192.168.0.28	5.7 Mb

Visited sites: list of IP addresses.

It lists the IP addresses that contain statistics on the sites visited by users. By selecting an IP address, it charges the tile with the list of the top 100 most visited websites highlighting on the right the generated traffic.

The value of the generated traffic assumes the following colors:

- White: if traffic is less than twenty five MB;
- Brown: if traffic is more than twenty five MB and less than one hundred MB;
- Red: if traffic is higher than one hundred MB.

Prime 100 siti più visitati
Elenco siti web con byte e hits

Tutte le ore

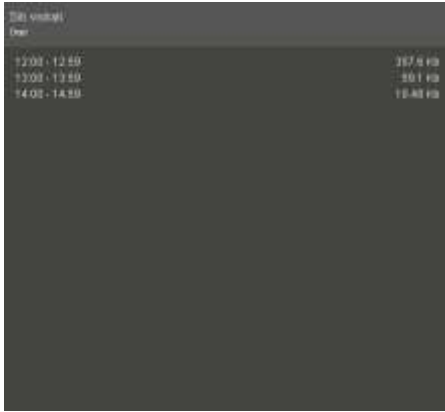
maps.google.com	378.87 Kb
www.libero.it	127.96 Kb
lrplug.it	98.3 Kb
www.google.com	86.58 Kb
maps.gstatic.com	69.87 Kb
italiaonline-d.openx.net	53.57 Kb
lplug.it	38.71 Kb
d3sxcf6d4fxjg9.cloudfront.net	20.49 Kb
u.openx.net	17.63 Kb
17.252.27.246.443	15.76 Kb
fonts.gstatic.com	13.59 Kb
web.whatsapp.com	10.97 Kb
maps.googleapis.com	7.86 Kb
d3ujb29x3alxd.cloudfront.net	7.39 Kb
dp.g.doubleclick.net	6.81 Kb

Visited sites: list of the top 100 most visited websites.

It lists the top 100 websites visited during the selected date and IP address, highlighting on the right the number of Hits (number of performed logins) and developed traffic.

By selecting a website, it reloads the tile with the times.

The combo box at the top-right on the tile allows you to filter the websites that have made traffic during the selected time band.




Time Band	Traffic
12:00 - 12:59	2074 hits
13:00 - 13:59	2011 hits
14:00 - 14:59	1843 hits


Visited websites: timetables.

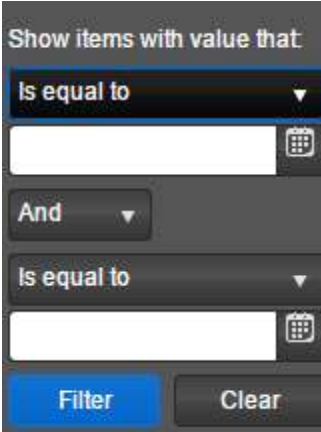
It lists the timetables on which traffic has been generated for the selected website highlighting on the right the traffic developed in the time band.

Tables

Tables contain a paginated list of information where you can perform searches to find specific records or sort data by column.

To search, even multi column, click the  symbol in correspondence of the column title you want to filter. After the click, the search options will display where you have to select the type of search (is equal to; not equal to; start with; contains; does not contain; ends with), the search text and the eventual combined or alternative search (and, or) submitted as for the preceding field. Once you have made your choices, to make your search effective, press the "Filter" button.

To disable a search previously activated, click the  symbol (the fact that it is highlighted in blue, means that it is active) and press "Remove".



Column filter for the tables


It is possible to change the sort order of the data in a table by clicking the title of the column to sort. By clicking again on the title, the arrangement will be changed in ascending. To disable sorting of the column, click once again.

If there are many data a layout will be visualized, namely a pagination of the first twenty, fifty or one hundred records, depending on the choice made.

It is possible to navigate from one page to another using the status bar at the bottom.



Table status bar


 Not in all the tables, you can perform searches and/or sorting.

Pages for Inserting or Editing

Web pages that allow you to insert or edit contents on textual and numeric fields, combo boxes, images, multi selection, etc.


These pages, further to other specific buttons, contain at the top-right in the "Commands" are, the "Save" button to save the inserted or edited data.





Context Menu

In almost all types of data, it is present the property button  that displays or hides the context menu, which allows access to specific context functionality.

The menu in its turn is divided into the following groups:

Title	Description
Edit	Groups options for the data editing. In addition to the standard ones described in the following paragraph, there are also included options to add new data.

Below you find some features of the contextual menu shared in many types of data and usually grouped under the " Edit" title, to which you will find references in the rest of the manual:

Option	Description
 Edit	Goes to the edit page of the data.  Available only if the user has permissions to read the current data.
 Delete	Deletes the current data.  Available only if the user has permissions to delete the current data.

First Login to the Administration Interface

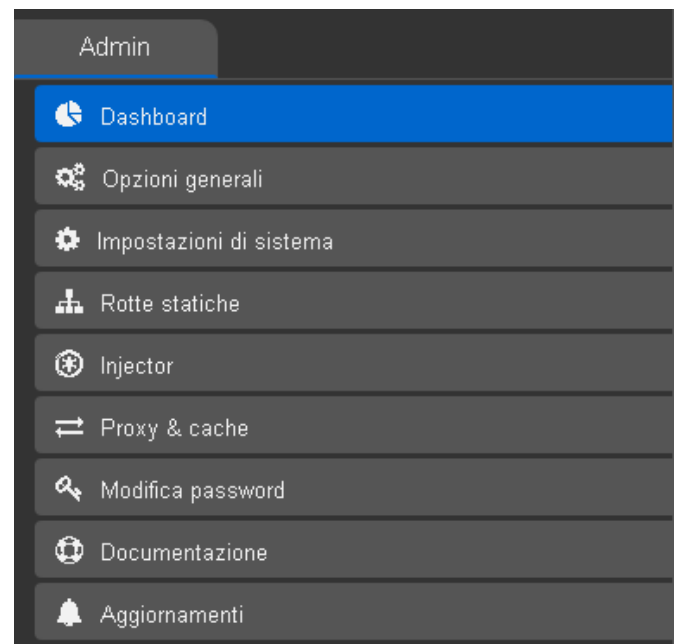
To log in the system for the first time and configure it according to your needs, open the web browser of the computer connected to CO.IN. and enter `http://192.168.168.10` in the address bar. The login page will appear in the CO.IN. Web management interface. Enter "0000" as "Password" and then press "Enter" or "Login" button.

The first task you have to perform is changing the admin password in order to customize it. Click on "🔑 Change password" in the sidebar. A new page will appear that allows you to enter your new password and to confirm it in the "Repeat Password" field. Then press on the "Save" button at the top-right to save and change the password of the Admin user.

✎ We suggest you keep your credentials safe, as they are the only ones that allow access to the appliance.

Assigning Network Parameters

To define the IP address to be assigned to the CO.IN. Ethernet interface and its network parameters, click on the "Admin" tab and select "⚙️ System Settings".



Configuration options for the administrator

✎ The default IP address 192.168.168.10 will remain configured for any emergency.

Follow these steps:

- Enter in the "IP Address" field, the IP address that you want to assign to CO.IN. so as to connect it to your network (e.g. 192.168.0.200);
- On "Subnet Mask", enter the network mask in CIDR format (example: 24);
- On "Gateway", enter the gateway of your network (e.g. 192.168.0.1);
- On "Primary DNS" and "Secondary DNS", enter valid DNSs (Example: 8.8.8.8 and 8.8.4.4);
- In the "Host Name" field, enter the name to assign to your device (example: CO.IN.).

Now on the upper right corner in the command bar, click on the "Save" button, and then on the "Restart Services" button so as to assign the new IP address.


Now you can log in the web administration interface of the appliance using either the IP address 192.168.168.10 or the new IP address and connecting it into your network switch.


Connecting to Your Network

Now you can connect the device to your network and verify if it is reachable by trying to access via web the set IP address (in case it is unreachable, you can always access through the IP address 192.168.168.10 by connecting a PC on the Ethernet port).

Updating the Software

We recommend you to update the CO.IN. software as to have the latest version including the updated manuals.

After having logged in the web administration interface, click on " [Updates](#)", then click on the "Update Now" button and confirm the update by pressing the "Ok" button.

 The update is available only if you are within the Software Maintenance and Update period or if you have purchased a Software Maintenance and Update contract for CO.IN. For more information, please contact your dealer.

Administering the System

Introduction

Below you can find in detail all the various features that are available in the options of the sidebar.

General Options

It allows you to define all the basic configuration data necessary for the proper functioning of the device.

Listed below you can find the manageable fields of this page.

General Info

Field	Description
Company Name	Enter the company name that owns CO.IN.
Address	Enter the address (e.g. 123 High street).
City	Enter the city.
Province or State	Enter the province or state.
Country	Select the country.
Phone	Enter the phone number (mobile or fixed).
Fax	Enter the fax number.
VAT-Id Number	Enter the VAT number.
Web Address	Website of the company that owns CO.IN.
Email Address	Email address of the company that owns CO.IN.

Logos for System Administration

Field	Description
General Image of Login	Image displayed in the login page to log in the management area. Dimensions must be 190 x 80 pixels.


System Settings


It allows you to define all "system" settings (network, web server, NTP, etc.) of CO.IN.

To make changes become effective on the various fields, you must press the "Save" button and in most cases, you will be prompted to restart the services by clicking the "Reboot Services" button.


Manageable fields of this page are as follows:



License

Field	Description
GUID	License identifier. Usually the license ID is already present and should not be modified otherwise there is a risk of the device malfunction.
Update License	<p>By clicking the "Update" button, you perform the immediate update of the license so as to enable new functionalities or new purchased modules. If you do not click it, the update will be anyway performed within eight hours.</p> <p>It is used also at the moment of the purchase of CO.IN., usually provided with minimum functionalities, in order to enable modules or the purchased model and associated to the GUID.</p> <p> Warning! Update can be performed only if CO.IN. is connected to the internet.</p>



 If the GUID is valid and if you have a "Software Maintenance and Update Contract", you can install software updates. The validation of a new GUID will be performed within 8 hours. Validation requires the connection to the internet.



Network

Field	Description
IP Address	<p>Enter the IPv4 address to be assigned to the device. As already explained we recommend you to assign a public IP address and possibly install the appliance in a DMZ. If you set up a private IP you will need to enter some redirects in your router firewall for the following ports:</p> <p>80 → web-based administration. 443 → web-based administration.</p> <p> Warning! In the system it is also preconfigured the IP 192.168.168.10 (not editable) assigned as additional IP. You can use this IP address in case the appliance is no longer reachable using the defined IP address.</p>
Subnet Mask	Enter the appliance network mask in the CIDR format (for example: 24 corresponds to 255.255.255.0; 16 corresponds to 255.255.0.0)
Gateway	Enter the IP address of the network gateway where CO.IN. is connected. It is the router IP address that allows connection to the internet.
Primary DNS	IP address of the primary DNS (mandatory).

	<p> Warning! Verify that the entered URL or IP points to a valid and functioning DNS otherwise the appliance will not work properly. If you do not know any DNS servers, use a public one such as 8.8.8.8.</p>
Secondary DNS	<p>Secondary DNS server IP address (mandatory).</p> <p> Warning! Verify that the entered URL or IP points to a valid and functioning DNS otherwise the appliance will not work properly. If you do not know any DNS servers, use a public one such as 8.8.8.8.</p>
Host Name	<p>Enter the host name to identify the appliance on your network. Note that this name is not already present in some other network device and it must not contain spaces and/or characters such as ?, ^, (,), etc.</p>

Web Server

Field	Description
Domain Name	<p>Domain name (e.g. www.domainname.it or coin1.domainname.it) on which it will be possible to reach the web administration interface. This domain must be properly registered at a Registrant and it must have the DNSs correctly configured. Otherwise, the web interface could not be reachable. In case it is possible to define as domain name the IP address with which it is possible to reach the device (e.g. public IP of the router WAN if it is private, or the IP address previously defined if it has been entered as public). It is recommended anyway to set up a domain name, even of third or fourth level.</p>
Administrator Email Address	<p>Enter the email address of the system administrator. This address will receive any system notification such as warnings or errors.</p> <p>It is also used as the sender when sending emails.</p>
Generate CSR Certificate	<p>Allows you to generate the CSR file (Certificate Signing Request) required to purchase a certificate from a CA (e.g. VeriSign). This procedure will automatically generate the KEY file (private key) that will be automatically uploaded in the appliance when you upload the corresponding CRT file issued by the CA. At the end of the procedure for generating the CSR, you will be allowed to save the file on your computer, and then you will have to edit the file, copy the entire contents and paste it into the web page of the CA certificate request. To generate the CSR file and the KEY file, click the "Generate CSR" button and save the file to use for the future certificate request to the CA.</p> <p>Warning: The CSR file is generated using the following fields previously set in the " <u>General Options</u>" page or " <u>System Settings</u>". We recommend you to generate the file .CSR only if these fields are definitive and will not be modified</p>

	<p>Country → General Options</p> <p>State/Province → General Options</p> <p>City → General Options</p> <p>Company Name → General Options</p> <p>Domain Name → System Settings</p> <p>Email Address → System Settings</p> <p>If you upload a certificate generated when the "Domain Name" is set to "coin1.domainname.it" and then you change the "Domain Name" to "coin2.domainname.com", the certificate would no longer be valid and the appliance would not be reachable.</p> <p>Initially, not being uploaded a certificate, if you try to log in in HTTPS to CO.IN., you will see the error "FORBIDDEN: You don't have permission to log in/on this server."</p>
Key File Certificate	KEY file certificate for SSL connections. If loaded with this option, overwrites the KEY file generated by the option 'Generate CSR'.
CRT File Certificate	CRT file certificate for SSL connections. Upload the CRT file issued by the CA. This file is closely related to the KEY file (private key) that has been automatically generated when generating the CSR. If the CRT file is not the one linked to the CSR and the KEY file generate by "Generate CSR certificate", it will not load a new certificate and will use the default ones. If the CRT file corresponds to the KEY file, certificates will be uploaded in the appliance configuration and you will be asked to restart the services. Then you will be able to access the administration appliance through HTTPS.
Trusted Intermediate Certificates CA	<p>CRT file containing the intermediate certificate/s. Import the certificate or the certificates of the intermediate certification authority (CA) if the certificate has been issued by an intermediate certification authority. You will be prompted to restart services.</p> <p> If you want to delete the CA's intermediate certificates, press the "Delete" button on the left.</p> <p> To enter more certificates of intermediate authorities, create a single file containing the various CRTs.</p>

Data Optimization



Field	Description
Keep the Traffic Logs for	Defines how long to keep the logs of the websites visited by users. The oldest logs will be deleted in order not to saturate the available disk space.


Email Messages


Field	Description
SMTP Server Address	Enter the address of the SMTP server that will be used for

	sending email notifications and/or warnings.
Enable SMTP Secure Connection	Allows you to enable secure connections (SSL or TLS) for SMTP. For Gmail, use SSL and port 465 and enable access to less secure App to URL https://www.google.com/settings/security/lesssecureapps . Possible options are: <ul style="list-style-type: none"> • No: does not enable SSL nor TLS • Yes with SSL: enables SSL • Yes with TLS: enables TLS
SMTP Port	Enter the SMTP port. Generally, it is the 25.
Enable SMTP Authentication	If enabled, enable SMTP authentication.
SMTP Username	SMTP username.
SMTP Password	SMTP password.

NTP

Field	Description
NTP Primary Server	Set the IP address of the primary NTP server for time synchronization system.  It depends on the value set in the “Timezone” field.
NTP Secondary Server	Set the IP address of the secondary NTP server for time synchronization system.  It depends on the value set in the “Timezone” field.
Timezone	Defines the timezone for HSNM.

 If CO.IN. is located behind a firewall, you will have to open the UDP 123 port to allow synchronizing the time of the device with the NTP server you have set.

 After setting the NTP server, by clicking the “Save” button, and then pressing on the “Reboot Services” button, time will be synchronized with the new NTP server you have set.

Injector

Through this page, you can enable the injector, which is the system that is able to insert contents in the pages visited by users.

Contents are provided by the advertising campaigns present in the HSNM and then it is necessary to enter the URLs or the necessary IPs to reach the HSNM or HSNMs.

The page allows you to manage the following fields:


Options

Field	Description
Enable	Enable or disable injection.


HSNM


The IPs or URLs specified in the following fields indicate to CO.IN. which is or which are the HSNMs that will provide injection contents. If more HSNMs are indicated it means that CO.IN. is configured in Round Robin to balance the workload of HSNMs and to achieve high availability.

Field	Description
URL 1	Defines the domain name of the first HSNM (e.g. hs1.domainname.it) to which the injection's requests will be direct.
URL 2	Defines the domain name of the second HSNM (e.g. hs2.domainname.it) to which the injection's requests will be direct.
URL 3	Defines the domain name of the third HSNM (e.g. hs3.domainname.it) to which the injection's requests will be direct.

 If CO.IN. is in the same network of one or more HSNMs and the HSNM or HSNMs are reachable by a domain, enter in the URL1, URL2 or URL3 fields, the private IP addresses of the HSNMs. In this case, the system will contact the HSNMs via IP, into giving the domain name defined in the System Settings of the HSNM, it will automatically create a match between IP addresses and domains in the system hosts file, in order to use the domains to reach the HSNM. After this processing, the values of the IPs will be overwritten by the corresponding domain names.


Static Routes

Through this page, you can enter static routes into the system (static route) needed to reach the unreachable networks through the default gateway set in the " [System Settings](#)" page.

The page displays a list of the static routes already entered. For each record, on the right, the context properties button  allows you to: edit a static route; delete a static route.


At the top-right, in the command area, the following button is present:

- Add

By pressing "Add" or by choosing " Edit" from the data's context menu, you can add or edit a static route. You will be redirected to the relevant entry page that allows you to process the following fields:

Data

Field	Description
Destination Address	Destination network address.
Subnet Mask	Subnet mask.
Gateway	Gateway.





 Example: if CO.IN. has the IP address 192.168.0.100 with gateway 192.168.0.1 and you want to reach the 10.0.0.0/24 network, you must insert a static route with destination address 10.0.0.0 subnet mask 255.255.255.0, and gateway 192.168.0.1.


⇄ Proxy & Cache

Through this page, you can define some Proxy related parameters inside the CO.IN. in order to tailor the product to meet your needs.


Manageable fields in this page are as follows:

Options

Field	Description
Enable Cache	<p>If enabled, it keeps in memory the most visited contents by users to provide them quickly and without consuming bandwidth.</p> <p>In other words, when enabled, it reduces traffic and repeated requests to the internet and the system can provide contents (if already present) directly to the users without contacting external servers.</p> <p>To improve users' browsing experience, it is recommended to enable this option.</p>
Enable on HTTPS	<p>If enabled, it uses proxy also for the HTTPS traffic and it allows performing the injection of contents even on protected pages.</p> <p>At the first run an authority certificate of CO.IN will be created in the path <code>http://DominioOIPdiCOIN/data/proxy.crt</code>. This CA is used to automatically generate SSL certificates of the sites viewed by users. Since users' browser does not recognize the CA that has issued the certificates, to the user will be displayed a warning message every time he visits a site based on HTTPS. To avoid this problem it is necessary to install in the users's system in the "Trusted Root Certification Authorities" the certificate available from the URL <code>http://DominioOIPdiCOIN/data/proxy.crt</code>.</p> <p> Warning! Some internet sites (i.e. facebook, twitter and dropbox) implement a security system called "Content Security Policy directive" that prevents the injection.</p> <p> Warning! In the HotSpot system, it is not recommended to use this option because clients should install a security certificate that can be downloaded from http://COINDomainOrIP/data/proxy.crt.</p> <p> If you enable this option in a HotSpot system, at the display of the Welcome Portal to the user, it shows a message that it is necessary to install a certificate and allows the download required for installation.</p> <p> Warning! Enabling HTTPS can cause problems with some services that do not use the standard HTTPS protocol on port</p>


	443. It might be necessary to enter the IPs, the classes and the domains used in the various services in the “Bypass Proxy” field.
Regenerate certificate	<p>Pressing the button “Ok”, allows to regenerate the certificate to be installed on users’ devices based on the information entered in the general options.</p> <p> Warning! If the certificate has already been installed by users, it has to be reinstalled again.</p>

Bypass Proxy

Field	Description
IP, Networks or Domains	<p>List of IP addresses, networks or domains separated by line breaks or comma whose traffic should not pass through proxy.</p> <p>Any networks must be entered in the form Network/CIDR prefix (e.g.: 100.101.102.0/24).</p> <p>Using Proxy with certain internet services non-HTTP defined or standard HTTPSs, can cause problems. This list allows bypassing the proxy for certain domains and/or IP addresses in order to directly divert the traffic developed towards these.</p> <p>Applications that can face problems are typically those of instant messaging, VoIP, VPN, remote control of computers, Play stores, App stores, online games, etc.</p> <p>The system, so as to avoid compatibility problems, automatically enters a bypass for the following applications:</p> <ul style="list-style-type: none"> • Skype • Whatsapp <p> If you want to post any comments, start the line with the # symbol.</p>


Binding IPs to Names

In this page you can bind the IP addresses, displayed in the dashboard, a name to better identify a client or an user to whom the IP is associated. In practice, if in a local network, the client 192.168.0.35 corresponds to the user John Doe, it is possible to enter the IP, first and last name so that, in the dashboard, it will be displayed John Doe (192.168.0.35).

The page displays a list of the bindings already entered. For each record, on the right, it is present the  property button that allows to: edit a binding; delete a binding.

At the top-right, in the command area, the following button is present:

- Add

By pressing “Add” or choosing " Edit” from the data’s contextual menu, you can add or edit a binding. Then you will be redirected to the entry page that allows to processing the following fields:

Data

Field	Description
IP Address	IP address to bind to a name.
Name	Name to bind to an IP address.

Antivirus

In this page you can decide whether to enable or disable the antivirus that allows protecting users from malicious contents present in the visited web pages.

Manageable fields on this page are as follows:

Options

Field	Description
Enable Antivirus	If enabled, it activate the antivirus for the pages visited by users.

If you have subscribed a contract of maintenance and upgrade of the CO.IN. system, the antivirus is updated automatically every day.

Blacklist

This feature allows you to block access to certain sites predefined and organized by category. The URL contents of the categories are constantly updated based on what reported by various supervisor associations and entered in CO.IN. by system updates.

Due to the propagation of malicious sites, with contents not suitable for minors or that you do not want to allow in the supplied service, it is a good practice to keep CO.IN. always up-to-date to the latest version.


I campi gestibili in questa pagina sono i seguenti:

Options

Field	Description
List of Provided Categories	If enabled, it blocks all sites provided by the category. In parentheses, next to the title, it shows the number of URLs or IP addresses that will be blocked.

Documentation

This page contains the list of the guides available for the use or the configuration of the device updated to the latest version.

 **Warning!** Documentation is dynamically downloaded from internet to the request. The device must be connected and configured to access the internet. If it is not possible, request documentation to the dealer.

Updates


CO.IN. is equipped with a system for updating in order to allow the distribution and installation of fixes and improvements. By accessing the page, an automatic comparison will be run between the appliance version and the latest published version in order to determine if there are any available updates.




If there are any available updates, you will see the message "A new version of the system has been released!" and a button saying "Upgrade now".


By clicking the "Upgrade now" button, upon confirmation, you run the download and automatic update of HSNM during which you will see the message "update in progress". After the upgrade, which can last a few minutes, you will see the message "your system is updated with the latest version available". In case there are no available updates, you will see the message "your system is updated with the latest available version".

In the middle of the page there will be reported the change log that contains all the news and/or bugs introduced/fixed in various versions, divide by date and version, in order that the CO.IN. administrator can evaluate if to upgrade or not.


To install an update, you must be in the warranty period of CO.IN. or to have undertaken a "Software Maintenance and Update Contract". For commercial information, please contact your dealer.

 To perform the update, the device must be connected to the internet in order it can reach the servers for the live update. The update takes place through the port 80, so it is recommended to open it in your firewall.

 Display of the page with updates may also fail in case of problems with the DNSs in resolving the names. In case of problems check the DNSs configured in " [System Settings](#)". To test the DNSs, open the " [System Information](#)" page and try some URLs in the "Ping" section.

 In the sidebar, the "Upgrade now" inscription may automatically change to "New version available". This happens when and if CO.IN. automatically detects updates.

In some conditions or when critical updates are released, you may be requested to perform one or more system updates (Apache, Proxy, Compiler or Kernel). It is recommended to install all the suggested updates.

 **Warning!** System updates may require a restart.

Activating CO.IN. in HSNM

To enable the injection in a gateway of the HSNM, please proceed as follows:

- Edit the gateway configurations (press “Edit” from the context menu of the gateway);
- In the “Injection” field, choose “Enable” or “Use domain settings”. In the latter case, you have to choose “Enable” in the same field of the domain’s data.
- In the “Injection” group, in the “CO.IN. Gateway GUID” field enter the CO.IN. GUID by copying it from the “System Settings” of CO.IN.;
- Define whether or not to display the toolbar that allows the user to go back to the Welcome Portal as to use the Apps or to disconnect;
- Press “Save” in the upper-right corner.

At this point injection is enabled and it is necessary to create an advertising campaign defining the fields for the injection. To do this insert an advertising campaign at “Gateway” or “Advertiser” level, define the general options and the various fields present in the “Injection” tab.

In the injection, you can enter the following types of contents:

- Image;
- YouTube Video;
- External URL (pages on other web servers)

It is possible to declare the placement (bottom, top, center and full screen), the size of the frame that displays the content and after how many seconds to display the button that allows the closure by the user.

Remote assistance request

When necessary and upon request it is possible to perform remote assistance by a technician certified in CO.IN. systems.

To enable his task, it is necessary that the appliance is connected to the internet through a static IP or to enable the port forwarding to the address 192.168.10.10 or to the one assigned to the device for the port 5900 (VNC) and 22 (SSH).

For any technical support request related to CO.IN., you can email to our technical team at support@hsnetworkmanager.com

Ports to open on your router/firewall

If CO.IN. is connected to a network protected by a firewall (for example on a DMZ) or on a private network LAN “natted” through a router, you will have to open the following ports for proper functioning:

Port N°	Protocol	Direction	Description
80	TCP/UDP	IN/OUT	Necessary in order to achieve via web the administration console.
443	TCP	IN/OUT	Necessary for example to PayPal in order to complete the payments.
21	TCP/UDP	IN/OUT	Necessary in order to install any software updates.
22	TCP/UDP	IN	Necessary for any remote assistance access.
23	TCP/UDP	OUT	Necessary for HSNM to hotspot connections (TELNET).
123	TCP/UDP	OUT	Necessary for clock synchronization.
5900	TCP/UDP	IN	Necessary for any remote assistance access.