

Colibri NetManager Platform

User's Guide

Copyright© Teldat-DM903-I Version 1.1, 2015 Teldat, S.A.

Legal Notice

Warranty

This publication is subject to change.

Teldat, S.A. offers no warranty whatsoever for information contained in this manual.

Teldat, S.A. is not liable for any direct, indirect, collateral, consequential or any other damage connected to the delivery, supply or use of this manual.

Table of Contents

Chapter 1	About this guide.	1
1.1	Supported devices	1
1.2	Who should read this manual?	1
1.3	When should I read this manual?	1
1.4	What is in this manual?	1
1.5	What is not in this manual?	1
1.6	Technical support.	1
1.7	Related documentation	2
Chapter 2	System overview	3
2.1	General description	3
2.2	Tool layout.	4
Chapter 3	Concepts and organizational elements	5
3.1	Users and permissions	5
3.1.1	New user profile	5
3.1.2	Creating a new user.	5
3.2	Devices	5
3.2.1	New device registration	6
3.2.2	How to determine whether a device is manageable	7
3.3	Device groups	8
3.3.1	How to create a device group	8
3.4	How to classify devices using tags	9
3.4.1	Assigning a tag to a device.	9
Chapter 4	Configuring access points	10
4.1	Defining a template for a basic access point setup	10
4.1.1	How to setup an access point from a configuration template	11
Chapter 5	Configuring routers	13
5.1	Handling text configurations	13
5.2	How to create a text configuration template	14
5.3	How to configure a router from a text configuration template	15
5.4	Updating the device configuration.	15

Chapter 6	Working with applications on application hosts	17
6.1	Installing applications	17
6.2	How applications are configured	17
6.3	Preparing the system for later deployment	18
Chapter 7	Monitoring.	19
7.1	Viewing the general system status	19
7.2	Getting the detailed device status	20
7.3	How to view detailed information for wireless clients	22
7.4	Setting rules for alerts	23
Chapter 8	Device positioning and maps.	25
8.1	How to set the device position	25
8.2	How to view devices on a map	25
8.3	How to configure floor plans	26
Chapter 9	Other management operations.	28
9.1	Processing alerts	28
9.2	Understanding the log section	28
9.3	Special operations	29
9.4	Device firmware upgrade	29
Chapter 10	How Teldat, S.A. licensing works	31
10.1	Requesting a new license	31
10.2	Activating a license	31
10.2.1	How to activate licenses for the cloud service.	31
10.2.2	How to activate a license for a virtual appliance installed in your data center	32
Appendix A	Troubleshooting.	33
A.1	Symptom: Cookies message	33
A.2	Symptom: The web site does not work.	34

Chapter 1 About this guide

This is the user's guide for the Colibri NetManager platform. The Colibri NetManager platform is a software tool for managing different kinds of network devices using a centralized approach.

1.1 Supported devices

The Colibri NetManager platform currently supports the following devices:

The **ATLAS360, ATLAS260, ATLAS160, VyDa4M, ATLAS60, ATLASi60, Teldat M1, Teldat H1, Teldat L1+, Teldat H1 Auto+, Teldat H1 Rail, Teldat H4, Teldat K** and the **Teldat V** router families.

1.2 Who should read this manual?

This manual should be read by users who will be using the Colibri NetManager platform.

1.3 When should I read this manual?

Read this guide once you have registered on the Colibri NetManager platform and received the account activation email. This manual explains how to add devices to the platform and the management operations that can be carried out over the devices.

1.4 What is in this manual?

This user's guide contains the following information:

- An overview of the Colibri NetManager platform software.
- Main concepts and organizational elements of the software.
- How to setup an access point with basic settings.
- How to generically configure routers.
- How to install and configure applications on an application host.
- How to monitor the devices, plus the parameters that can be monitored.
- How to place devices on maps and floor plans.
- Other useful management operations.
- Troubleshooting when accessing the platform from a browser.

1.5 What is not in this manual?

This manual does not contain information relating to device hardware. While it explains all the main operations, it is not intended as a comprehensive guide to all management operations available on the platform. This manual does not contain information on how to setup devices for Internet connection. For further information on configuring the device, please see the relevant manuals for the different devices at the following website: www.teldat.com.

1.6 Technical support

Teldat, S.A. offers a technical support service. Regular device and server software updates are available for maintenance reasons and new features.

Contact information:

Web: www.teldat.com

Tel.: +34 918 076 565

Fax: +34 918 076 566

Email: support@teldat.com

**Note**

The manufacturer reserves the right to make changes and/or improvements to the software, hardware and documentation without prior notice. The screen captures shown throughout the guide are provided for information purposes only. Some small modifications may exist in the current software.

1.7 Related documentation

Colibri Management Platform Administrator's Guide.

Colibri Management Platform User's Guide.

Chapter 2 System overview

2.1 General description

The Colibri NetManager platform is a software tool for network device management. It can either be installed on the existing customer data center infrastructure (*Virtual Appliance*) or be used as a cloud service provided by Teldat, S.A.

In both cases all the features and functionalities are the same.

Colibri NetManager includes configuring and monitoring functions and generates usage and incident reports during the device management process.

The platform can be accessed universally through any JavaScript-enabled web browser. In particular, Firefox, Chrome, Internet Explorer 8 (or above) and Safari browsers are supported.

To enter the platform the user should type the <https://teldat.networkcloudmanager.com> URL into the address bar of the browser they wish to use.



A new customer must register from the login screen. This is done by clicking **Register** at the top of the screen on the right and creating an account and an associated administrator user.

Once the customer has registered, an activation email is sent to the email account provided. Following activation, the user will need to setup the access password for subsequent logins.

Once the account is activated, the user can access the platform by entering his/her credentials in the login screen.

You must purchase licenses in order to manage devices. The licenses purchased for the cloud service are valid for a minimum of one year.

Please contact your distributor if you have any queries concerning the available licenses or how to purchase them.

Control connections between devices and the management platform are always initiated by the devices, resulting in a very flexible architecture. Thus, with Internet access (or data center access in the case of a private cloud) the device sets up a secure SSL channel for the exchange of management messages.

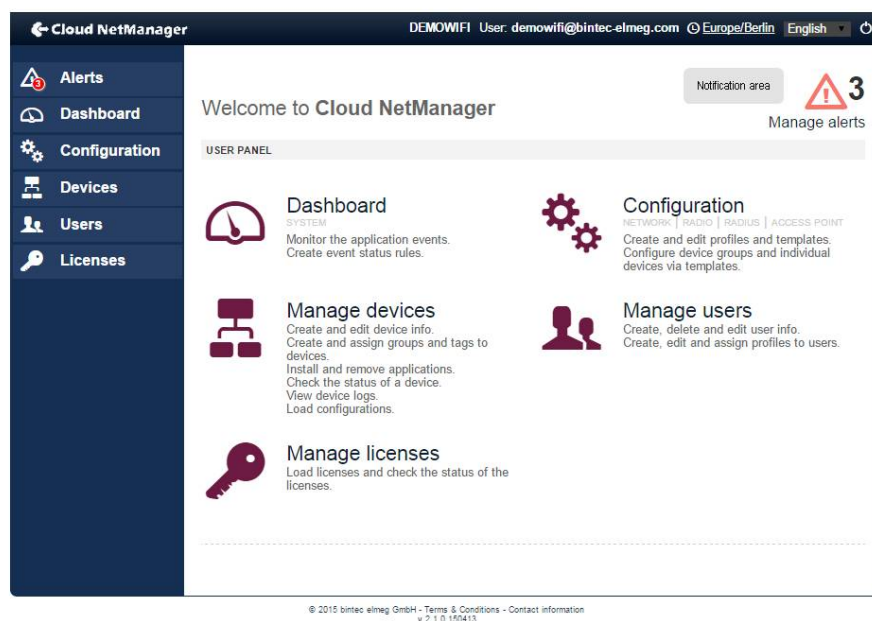
Both SSL server certificates and SSL client certificates are used to establish the connection. This ensures maximum security in data transmission as all messages are encrypted.

Device data traffic does not reach the management platform, thus ensuring that the solution is fully scalable.

Using our platform software as a service you not only benefit from the highest level of availability but also gain immediate access to the latest software upgrades and functionalities.

2.2 Tool layout

The tool is divided into several sections providing an organized and user-friendly format for device management and monitoring.



The selection menu is shown on the left-hand side. Click on each option to access the corresponding tool:

- **Alerts:** accesses alert visualization and processing.
- **Dashboard:** accesses hierarchical monitoring dashboards.
- **Configuration:** accesses configuration profiles and configuration templates.
- **Devices:** accesses the device management section.
- **Users:** accesses user registration and user permission configuration.
- **Licenses:** accesses the license registration and license status section.

The center is taken up by a panel that holds the GUI elements for each section. If you have not selected anything, you can select the icons and links displayed in the central panel to access the same sections as those appearing in the menu on the left.

The top right-hand area of the center panel is intended for notifications. The notification area holds various visual elements depending on the section, such as, for example, the number of pending alerts or the connectivity status of a managed device.

The status bar at the top of the tool displays the currently logged in user name, the selected time zone and the language selector. The disconnect button used to leave the tool and return to the login screen is found to the right of the status bar.

Chapter 3 Concepts and organizational elements

Several entities on the platform show the organization of the tool and the management and monitoring operations:

- **Customer:** this is the entity defining a management environment with access to a given set of devices.
- **User:** this is the entity featuring a tool user with a given set of permissions to operate the tool including access to given sets of devices.
- **Device:** this is the entity representing the managed network device.
- **Group:** this is the entity representing a group of devices. A device can only belong to one device group.
- **Tag:** this is an entity to classify devices. Each device can have a number of associated tags.

3.1 Users and permissions

Users who will manage and operate current customer devices are defined through the **Users** menu entry.

The user who registers the account and who is therefore the account administrator, must first set up the profiles for all additional users that will operate the platform.

3.1.1 New user profile

Select **Users|Profiles** to access the current list of profiles.

To create a new profile select **Users|Profiles|New Profile**.

First, you need to enter a name for the user profile you are creating. Next, select the set of platform operations that the user can access by checking the corresponding boxes of the desired operations.

Following this, select the **HomePage**. This is the initial screen the user sees when he logs on to the platform. In **Allowed device types**, select the type of devices the user can access and in **Allowed groups**, select the groups of devices that a user with this profile can access.

3.1.2 Creating a new user

Select **Users|New User** to access the new user form.

Enter the following in this form:

- **UserName:** this is the name that the customer user uses to access the platform (the username should match the email address described and entered below).
- **Profile:** this is the 'profile' assigned to the new user and features their access permissions.
- **Name and surname:** user's first name and surname.
- **Email:** user's email address.
- **Send registration email:** check this box if you want the user to receive an email once the account has been created on the platform.
- **Password / Repeat password:** enter the initial password that the new user uses to enter the platform. Type in the password again to check for mistakes. The user can change the password at a later date if required.

3.2 Devices

Devices (or equipment) are undoubtedly the central element of the platform.

Click on **Devices** to see a table containing the devices currently registered on the platform.

You must first purchase licenses before you can register devices. Please see *DM902: Getting started with the Colibri Platform* for a description on how to receive the purchased licenses and how to activate them in your management platform account. Once you have activated one or more licenses you can start reading the section on how

to register your devices.

3.2.1 New device registration

There are several ways to register a device on the platform. This goes from fully automatic mechanisms to manual mechanisms for inventoried devices.

Click on **Devices|Add devices** to get a screen where you can access the different device registration methods.


- **Discovered devices:** this section displays a list of discovered devices that have reached the platform but have not yet been 'claimed' by a customer.

To claim a device from this list you need to know its DVC (device verification code), which is marked on the device label. Using the DVC ensures that you are the owner of the device and that you have access to it.

Please locate the device DVC on the label. This is a 4 digit code e.g. DVC : 4567

Click the arrow on the far right of each row in the list to get a window with a lock code field. Enter the DVC code and click the + icon. The device is subsequently added to your list of managed devices and removed from the discovered devices table.

- **Manual registration:** this section allows you to manually register a device or batch of devices. Before you do this, however, you must obtain the serial numbers and DVCs of the devices you wish to register.

	<p>Important</p> <p>The devices do not need to be connected to the management platform in order to perform manual registrations.</p>
-----------------------------------------------------------------------------------	---------------------------------------------------------------------------------------------------------------------------------------------

Add devices - Manual registration

Parameter	Description
Mode	Select Enter serial numbers manually for a reduced set of devices of the same type. Select Enter devices from data source (.csv) for a large set of devices. In this case, you need to provide a comma-separated values file with a list of the devices to be registered.
Serial Numbers	If you have chosen to enter the serial numbers manually, enter the list of new devices to be registered in this box.
CSV file	If you have chosen to enter the serial numbers from a data source, select the local .csv file containing the list of devices.
Device Verification Codes (DVC)	Select the CSV column number containing the DVCs for each device.
Type*	Select the type of devices you are entering.
Name*	Enter a name for the new devices.
Description*	Enter a description for the new devices.
IP*	Enter a default IP management address for the devices.

* When importing devices from a data source you can use the icon to the right of the input field to assign CSV column numbers to parameters in the form.

- **Automatic registration:** this section displays instructions on how to setup your system to automatically register devices on the platform.

Automatic registration is the first step towards full zero-touch device deployment; i.e., an unboxed factory device can be wired in at its final location, connect to the management platform, retrieve its configuration and start operating without requiring any operator involvement other than the physical wire connections and checking that the device is powered-on and working.

Automatic registration is based on the DHCP protocol. If the deployed device obtains its network configuration from a DHCP server, the DHCP option 43 can be used to setup the management platform URL and the customer ID of the device owner.

An example of option 43 is as follows:


```
mngplat:url=https://Teldat.networkcloudmanager.com/AppAdminWeb/register.jsp?
uuid=7d87486c-646c-4358-bd2b-5c3165177290
```

To setup the DHCP server to enable automatic registration, please follow the instructions included on the platform for this section.

Teldat, S.A. access points come with a factory setup and with the following URL as the predefined management platform server address:

```
https://discover.networkcloudmanager.com
```

The device will replace this URL if it receives another one from the DHCP server. The devices will try to connect to the cloud service if you do not configure a specific management URL for the DHCP server. Furthermore, if the devices are able to connect to the server, they are listed in the **Discovered devices** section.



Important

If your management server host address includes a host name (this is default), the device should also receive the *DNS (Domain Name System) server address* from the DHCP server to be used, in order to resolve the host name for an IP address. This is necessary for the device to connect to the management platform and be managed.

3.2.2 How to determine whether a device is manageable

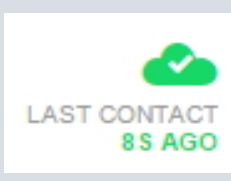
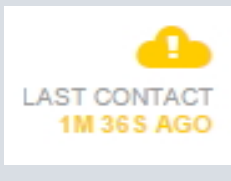
A device must contact the server periodically in order to be managed.

Once you have registered a device you can access the management sections for that specific device by selecting **Devices** and clicking on the row that contains the device.

The **Info** section displays an image of the device together with additional information on the device model, licenses and firmware release.

The notification area (in the top right-hand corner of the center panel) displays a cloud icon in different colors depending on when the device last contacted the server.

Device management - States

Icon	Device state	Description
	Managed	The device has contacted the server within the last minute and a half and can be managed normally.
	Loss of contact	The device has not contacted the server for more than a minute and a half. It may have lost the connection or be switched off.

	Disconnected	The device has not contacted the server for more than three minutes and cannot be managed.
	Never connected	The device has never contacted the server.

When a device goes into a *Disconnected* state, an alert is raised and the configured actions are carried out.

3.3 Device groups

Device groups are a key element of device management and monitoring.

This is because a major goal and design principle of the Colibri NetManager platform is to make the operations performed on devices sharing a common set of operating features as easy as possible.

Therefore, the first step towards management and monitoring of batch operations is the definition of a device **Group**.

3.3.1 How to create a device group

A new device group can be created in two ways:

- Globally, from the Group management section.

Select **Devices|Groups|New group**: A form will appear in which you can define the different parameters of the new group:

New group

Parameter	Description
Name	Enter a name for the new device group.
Description	Enter a meaningful description for the new device group.
Configuration template	Select the device configuration template that will be associated with the devices in the group. You can define a different template for each device type in the group.
Monitoring period	Setup how often (in seconds) the devices in the group will update their status information.
Automatic update	Specify whether the configuration of the devices in the group will be automatically updated when their configuration templates change.



Important

Take care when checking the **Automatic update** option since incorrect use can cause a large number of devices to lose the connection to the server and consequently become unmanageable.

- Device based, from the Device management section:

Select **Devices** and click on the device that you want to create the group for in the device table.

Select **Details|Group|+** and a window opens. Select **New group** and enter the name of the group you wish to create in the **Name** box. By clicking **Assign Group**, the group is created and the devices are included within the group. The group is initially created with certain default parameters. These can be changed later in the Group management section, as described in the above paragraph.

3.4 How to classify devices using tags

Tags are very flexible mechanisms for classifying devices. A device may have multiple **tags** and the same **tag** may be linked to multiple devices.

Tags are primarily used to make selecting devices easier for device monitoring and batch operations.

3.4.1 Assigning a tag to a device

Tags must first be created before they can be assigned to a device. To create a new tag select **Devices|Tags|New tag**. Enter a name for the tag and click on **New Tag**. The tag is now ready for use.

Select one or more devices from the **Devices** section. Click on the tag icon, select the tag you wish to assign to the device(s) and click **Assign tag**.

Once a tag has been successfully assigned, a group of devices with a tag can be selected by clicking on the funnel icon (usually filter) and choosing the desired tag(s).

Chapter 4 Configuring access points

To setup an access point, you must choose which *Configuration template* to apply. A configuration template is a group of parameters that can also include references to other groups of parameters. These groups of parameters are called *parameter Profiles*. A template defines the whole configuration of the device, although there are some optional profiles.

The profiles involved in an access point configuration template are:

- **Configuration|WLAN Profiles|Network**: Groups all the parameters configuring a wireless network. This includes the network SSID, network security setup, quality of service and VLAN tagging.
- **Configuration|WLAN Profiles|Radio**: Groups all the parameters configuring an access point radio interface. This includes the radio band and mode, the country in which the access point is operating and other performance and advanced parameters.
- **Configuration|WLAN Profiles|Radius**: Groups the parameters configuring the access point accessing a radius server for authentication. This is optional. It is only required when the security setup for any of the wireless network profiles in use with this access point is **WPA enterprise**.

The next section provides a quick configuration example of an access point.



Important

In-line help has been added to each parameter appearing in the different configuration forms and is displayed when you place your mouse over the parameter name.

4.1 Defining a template for a basic access point setup

In order to implement an access point configuration template, you must define at least one wireless network configuration profile and one radio configuration profile.

The steps required to perform a basic configuration are:

- (1) Create a wireless network profile:
 - Select **Configuration|WLAN Profiles|Network|NEW NETWORK PROFILE**. Enter a name for the profile you are creating in the **Profile name** box. This name uniquely identifies this group of parameters.
 - In the **Network name (SSID)** box, enter a name for the network. This name is the wireless network name for the end user wireless devices.
 - Specify the security schema to use; e. g., select **WPA PSK** in the **Security mode** box from the **Security settings** section. For this security mode, you also need to enter the password that users enter when connecting to the network. Enter the desired value in the **Secret** box.
 - Click on **New network profile** to finish creating the wireless network and then use the created network profile name to publish the network in a radio interface.
- (2) Create a radio profile:
 - Select **Configuration|WLAN Profiles|Radio|NEW RADIO PROFILE**. Enter a name for the profile in the **Profile name** box. Again, this name uniquely identifies this parameter group in the device configuration template.
 - Select **Access Point** from the **Operation mode** box. Click on the pull-down list beside the country parameter and select the country corresponding to the access point location. This is important in order to comply with different country laws regarding the transmission power and radio channels allowed.
 - Click on **New radio Profile** to finish creating the radio profile configuration.
- (3) Create an access point configuration template:
 - Select **Configuration|Device Templates|Access Point|NEW ACCESS POINT TEMPLATE**. Enter a name for the template in the **Template name** box. This name is used when assigning this configuration template to a group of access points.
 - For security reasons you must also enter a password in the **Administrative password** box. This is the new password that the *admin* user will need to enter to access the device's local web GUI.
 - To complete the configuration please click on the **Radio Module 1|Radio profile** pull-down menu and select the radio profile you created in paragraph 2. You must also click on the **Radio Module 1|Network profile** menu and select the wireless network profile that was created in paragraph 1.

Finally click on **New Access Point template** to create the new device configuration template.

4.1.1 How to setup an access point from a configuration template

Once you have defined the desired parameters and put them together in a configuration template, you must learn how to configure the access points with all the parameters.

To setup an access point, it must be included in a group. If you have not yet created a group, please read [Device groups](#) on page 8 to learn how to create a group of devices.

When you create a group or edit a previously created group (by clicking on **Edit group**), you can define the default configuration template assigned to the group's access points. To do this click on the **Configuration Template|Access Point** menu and select the configuration template created in paragraph 3 of the previous section.

Next, click on **Save changes** to permanently apply the configuration template to the group.

The length of time that the configuration is applied to the devices depends on the group parameters and the user operation.

- If the **Automatic update** box is checked for the group, configuration updates of all the group's access points are scheduled and started as soon as the configuration template has been assigned to the group and the changes saved.
- If the **Automatic update** box is not checked for the group, the configuration of the access points is not updated automatically and the operator is responsible for choosing when and which devices to update.

The operator can choose between a number of different operating procedures when scheduling updates for the configuration of the access points:

- (a) Immediately update all devices in a group:

Select **Devices|Groups** and click on the group that contains the devices you wish to update. Click on **Update configuration** to begin updating the configuration of the access points in the group.

- (b) Schedule an update for all devices, or a set of devices, at a given time:

In the **Devices** section, select the devices with the configuration you wish to update. You have several choices here: with a small number of devices you can carry out an individual search for each and check the selection box located to the left of the device in the **SN/MAC** column.

If you need to update a large number of devices, you can use the selection filters that appear when you click on the funnel icon (filter icon) situated above the device table. For example, you can preselect all the devices in a group by clicking on the corresponding group tag. Once preselected, you can mark and select the devices by clicking the check box situated to the left of the **SN/MAC** column. If you wish to exclude certain devices that have been selected, go to the row in which the device appears and click on the check box to uncheck it.

Once you have selected your desired devices, click on **Devices|BATCH OPERATIONS** in the device table heading and choose **Update System Configuration** from the pop up screen.

Click on **Start Wizard** to start the configuration update schedule. If you want the update to start immediately, click on **Apply** and leave blank the **As soon as possible** option that appears by default.

If you wish to schedule the update to take place at a given time, click on the **As soon as possible** field. Select **Scheduled** from the pull-down selection box and select the time of day that you wish the configuration update to take place in the hour/minute boxes.

Click on **OK** and then on **Apply**. The configuration update is now scheduled to take place at the specified time.

- (c) Update a single device:

To re-configure a single device, first go to the **Devices** section, click on the device row and select the **Configuration** section.

Click on **Send configuration** at the bottom of the screen to start the configuration update immediately.

**Important**

Devices must be 'connected' to the server in order to successfully perform any of the existing procedures for scheduling device configuration updates. When selecting the device, therefore, the icon in the notification area must display a green cloud. If a green cloud is not displayed, the device is not reaching the server and the operation cannot be performed.

You can view the progress of update operations for any update procedures by selecting **Devices**, clicking on the row in which the device appears and selecting the **Jobs|Show details** section.

Chapter 5 Configuring routers

The configuration of these kinds of devices is based on text mode configuration templates with a set of commands complying with the Teldat Router CLI (Command Line Interpreter).

5.1 Handling text configurations

Text configurations can be created using either an external text editor or the internal Colibri NetManager platform editor.

To write a configuration you need to know the syntax and the managed entities on the device. For example, a basic configuration for a Teldat router looks like this:

```
; Showing Menu and Submenus Configuration for access-level 15 ...

log-command-errors
no configuration
set inactivity-timer disabled
set data-link at cellular0/0
set data-link at cellular0/1
feature access-lists
; -- Access Lists user configuration --
    access-list 103
        entry 1000 default
        entry 1000 permit
;
    exit
;
exit
;
feature management-platform
; -- MANAGEMENT PLATFORM configuration --
    server colibri
        address teldat.networkcloudmanager.com
        enable
    exit
;
exit
;
;
network ethernet0/1
; -- Ethernet Interface User Configuration --
    ip address 172.24.0.93 255.255.0.0
;
exit
;
network ethernet0/2
; -- Ethernet Interface User Configuration --
    ip access-group 103 in
;
    ip address 10.1.1.2 255.255.255.0
;
;
repeater-switch
; -- Switch User Config --
    port 1 qos rate-limit 1
exit
```

```

;
  exit
;
  feature netflow
    ip export version 5
  exit
;
  protocol ip
; -- Internet protocol user configuration --
    route 192.168.212.0 255.255.254.0 172.24.0.245
    route 0.0.0.0 0.0.0.0 172.24.0.98
;
    classless
      nat pat
; -- NAT configuration --
      number-of-ports 32000
    exit
;
    proxy-igmp
; -- IGMP proxy user configuration --
      enable
    exit
;
  exit
;
  feature ntp
; -- NTP Protocol user configuration --
    protocol
    peer address 1 77.226.246.115
  exit
;
  feature dns
; -- DNS resolver user configuration --
    server 8.8.8.8
  exit
;
  dump-command-errors
end

```

To access the device configuration stored in the platform server, select **Devices**, click on the desired device and click on the **Configuration** section.

If the device was not configured from the management platform, the box where the configuration is usually displayed may be empty.

If you edit the configuration box in order to enter some configuration commands, or if you paste a configuration from an external text editor, you can send that configuration to the device by clicking on **Configuration|Send configuration**. This causes the device to download and apply the new configuration and stores the updated configuration on the DataBase platform.

As with access points, you can check the progress of a configuration update by selecting **Devices**, clicking on the given device and selecting the **Jobs|Show details** screen.

5.2 How to create a text configuration template

The same configuration structure will often be shared by a large number of devices from a particular customer, even if they are routers. This is because they are to be used for the same service.

The best way forward in these cases from a management perspective is to create a text configuration template where the device dependent parameters appear as variables and are assigned different values depending on the

device.

Creating a text configuration template is very easy with the Colibri NetManager platform. There are two ways to do it:

- From a device's text configuration:

Select **Devices**, click on the corresponding device and click on the **Configuration** section.

To create the configuration template from the current device configuration click on **Configuration|Save as template**. This will take you to the text template editor described in the following paragraph.

- From the text template editor:

Click on the **Devices|Configuration templates** to access the text template editor section.

If you wish to create a new text template, click on **New template**. In the **Name** box enter a name for the template and in the **Description** box enter a descriptive sentence.

The **Template Text** box should contain the start text configuration for the template. If you arrived here from a device's configuration section, this box should contain the selected device's configuration.

To include variables in the template you must replace the variable parameters with expressions such as **{{var}}**, where **var** is a variable name that is substituted for different values depending on the device.

Let's consider making the network interface IP address variable. In a given device, this is as follows:

```
network ethernet0/1
; -- Ethernet Interface User Configuration --
    ip address 172.24.0.93 255.255.0.0
;
exit
```

From the editor, replace 172.24.0.93 with the expression **{{ip_address_wan}}**. This results in:

```
network ethernet0/1
; -- Ethernet Interface User Configuration --
    ip address {{ip_address_wan}} 255.255.0.0
;
exit
```

When you have parametrized all the variables click **New template** to save the new text configuration template.

5.3 How to configure a router from a text configuration template

When you have a parametrized text configuration template you can use it to setup several devices.

To do this you will need an inventory file with all the serial numbers of the devices you wish to configure and the final values that each template variable in the text configuration template should have for each device.

This inventory file should be in CSV (comma-separated values) format. A CSV file for setting up two devices from a text configuration template with a variable called **{{ip_address_wan}}** would look like this:

Apply template - Table format

serial_number	ip_address_wan
757/00120	172.24.0.87
757/00113	172.24.0.100

Or its equivalent in CSV format:

```
serial_number;ip_address_wan
757/00120;172.24.0.87
757/00113;172.24.0.100
```

5.4 Updating the device configuration

Device configuration updates from a text configuration file can be scheduled to take place either immediately or at a given time:

(a) Immediately:

To schedule a configuration update to start immediately, select **Devices|Configuration templates** and click on the template you wish to use to configure the device. Click on **Apply template** and select the CSV inventory file using the format described above.

Next, click on **Upload CSV**. An information screen is then displayed where you will be able to view any problems that occur when processing the variables in the inventory file. You will also be able to check the resulting configuration for each device.

Click on **Assign template** to schedule an immediate configuration update for each of the selected devices. You can check the progress of the configuration update in the **Jobs** section of the devices.

(b) At a given time:

Select the devices that you want to update from the **Devices** table and click on **BATCH OPERATIONS**.

Next, select **New system configuration** and select the **Router** check box.

Click on **Start wizard** and the configuration wizard will guide you through the various steps.

Select the text configuration template name you wish to apply from the **Select a template** box. Then click on **Select file** to select the inventory file from which the device-specific configuration parameters are extracted.

The format of your inventory file may be multi-purpose and contain columns with additional parameters or information. Consequently, for each configuration template variable, you will need to select the CSV column number where the data for that variable is taken from the CSV.

Click on **Preview** to view the resulting text configuration after substituting each variable through its value.

If everything is correct and you wish to schedule the update to take place at a specific time, click on the **As soon as possible** link and select the time at which you want the update to be performed.

Finally, click on **Apply** to schedule the update.

Chapter 6 Working with applications on application hosts

The Colibri NetManager platform includes features to install/uninstall and configure applications on Teldat, S.A. multi-core devices with support for modular applications.

These kinds of devices are called **application hosts** within the platform.




You can access an application's icon from the Colibri NetManager platform. Applications have been developed by Teldat or third parties for these kinds of devices. Some application examples include: Network file server, Web cache, IP Cameras video recording, Proxy for Real time video streaming, etc. The Colibri NetManager platform is the only way to install applications on an application host.

6.1 Installing applications

Your application host device is ready to download applications once it has connected to the Colibri NetManager platform. Select the **Devices** menu option and click on the desired device from the device list and select the **Applications** section.

The "Installed applications" view is selected by default. Initially you will see an empty table since no applications have been installed on your device yet.

Applications - Views

Icon	View	Description
	Installed applications	Shows the list of applications currently installed on the device.
	Scheduled operations	Shows the list of applications pending installation/uninstallation from the device.
	Available applications	Shows the applications available for installation on the device.

Select the 4 rectangles icon from the top-right hand side of the applications list to obtain the Available applications view. A window will appear showing the available applications. Bear in mind that the applications shown may vary depending on the licenses purchased.

Click on the application for which you want to install a description to get the available releases.

Select a release and click on the **Install** button. Following a short pause, the application will be downloaded and installed on your device. You can repeat this process for each desired application.

Click on the **Pending Applications** icon during this process to see the set of applications that you have selected for this device that are pending installation.

The **Job** tab can be used to track the installation progress.

Once the installation process has finished and the application is properly installed, the **Application properly installed** message is displayed in the **Jobs** tab.

The application is now ready to be used in your device.

6.2 How applications are configured

The mechanisms described in [Configuring routers](#) on page 13 also apply to configuring applications, since the configuration of each application is handled with a text syntax similar to the router's CLI.


To start configuring an application installed on a device, first select the device by clicking on **Devices**, then search for it in the list and click on the row in which the device appears to access the device management section.

The system configuration is managed from the **Configuration** section of the device. As with the routers, you can define text configuration templates and apply them to a group of devices using variables and inventory files.

However, each application has its own configuration as well as a text configuration. To access a particular application's configuration, you must enter the device's **Applications** section and select the application you wish to configure from the Installed applications view.

To access the application text configuration click on **Configuration**. An editing box appears where you can enter/edit or paste the desired configuration.

Once you have the desired configuration click on **Send configuration** to update the application configuration running on the device.



Important

Please note that in order to update an application, the device must be connected to the server. When selecting the device, the notification area icon must show a green cloud as a reminder.

6.3 Preparing the system for later deployment

A group of devices can be setup for later deployment through the **Batch operations** button in the device table.

The **Batch operations** feature starts automatically after doing either of the following : answering **Yes** to a question such as "Would you like to configure the created devices"; after you have added new devices, or, pressing the **Batch operations** button when an existing group of devices is selected in the device table.

On the **Batch operations** form select **Install/Uninstall applications**.

Then click on **Start wizard**.

Click on the + icon at the bottom right-hand side of the application image to **provide** (schedule the installation) the group of devices with some of the available applications. The number of available licenses appear beside the + icon. Please make sure that you have enough licenses to cover all the devices, otherwise the process may fail for some of them.

Click on the - icon at the bottom left-hand side of the application image to remove the application from devices in the group of selected devices.

You can view a summary of the scheduled operations for each device by clicking on the **Preview** button. A label for each operation is shown to the right of the devices. Green means that everything is running smoothly, while Red, Blue and Orange alert you to errors or warnings during the running of scheduled operations. You can obtain information on an error or warning by placing the mouse cursor over the colored label.

The batch operation can be scheduled to take place as soon as possible or at a specific time. If it is scheduled to take place at a specific time, the operation will start if the device connects within an hour after the scheduled time. If scheduled, this time interval is valid for any day after the operation is assigned to the group of devices and until the operation has completed (whether successfully or not).

A green **All steps done** notice appears at the top of the form once the operation has been assigned to indicate that the operation has been correctly scheduled.

Scheduled operations can be viewed in the **Scheduled operations** application view in the **Application** section of the device.

Chapter 7 Monitoring

Device monitoring is one of the Colibri NetManager platform's most remarkable features.

As a general rule, the CPU and memory usage are monitored for any kind of device.

In order to view the current CPU and memory usage for a given device, select **Devices** and then click on the device you wish to monitor. Next, click on **Health** to view the current values of the CPU, RAM and Flash memory usage.

7.1 Viewing the general system status

Select **Dashboards|SYSTEM** to access the main monitoring screen.

All the dashboards are arranged based on movable widgets.

The main dashboard screen is organized into four sections:

- (a) **Dashboard**: where the widgets with the monitored date are placed.
- (b) **Maps**: where you can access the location and floor maps.
- (c) **Analysis**: where you can monitor a specific device.
- (d) **Rules**: where rules are configured in order to generate alerts based on the conditions applied to the values of the monitored parameters.

The monitored parameters are visually arranged into several categories in the dashboard section which correspond to the logically related group of parameters.

The first category is always known as the **Custom view**. Only those parameters selected by the user are displayed in this group.

The second category, (**All**), includes all the available widgets for the current kind of device. Following these categories and depending on the type of device, you will find categories for **System**, **Security**, etc.

To include a widget in the **Custom view** category, click on the + sign that appears in the top right-hand corner of the widget you wish to include in the customized view.

A widget that is already included in the **Custom View** cannot be added again (the + sign does not appear). Consequently the widget frame has a dashed line drawn across it in the original category.

The dashboard section initially displays a number of widgets together with the general status of the selected devices or groups. This is known as **System view**.

Widgets appearing in the system view are:

System dashboard - Widgets

Name	Description
Number of devices	This shows the evolution, in time, of the number of managed devices of every type (routers, access points, etc.).
Number of devices chart	This shows the current device type ratio for the devices registered on the platform.
Critical alarms	Lists the critical alarms for the selected devices.
Warnings	Lists the current warnings (non-critical) for the selected devices.
Number of WLAN clients	Displays the total number of wireless clients connected to the selected wireless devices.

Disconnected devices	Lists the devices that are currently disconnected. These devices are not manageable and the platform is not receiving any monitoring data.
-----------------------------	--------------------------------------------------------------------------------------------------------------------------------------------

7.2 Getting the detailed device status

You can access the **detailed view** of a device by clicking on the **Dashboard Analysis** section.

The table displays a list of specific types of devices. There are some buttons that act as filters for the different device types in the top row.

The device types are:

- Router:** By clicking on this button you can select the router devices.
- WLAN Controller:** Select and view wireless LAN controller devices only.
- Access Point:** Select and view access point devices only.
- Client:** Select and view the client devices that are wirelessly connected to any of the access points managed from the platform.

The search box, filtering button and links to select the time interval, situated above the table, make it very easy to search for and select devices.

The **Analysis** table displays a number of parameters for each listed device. The selected devices may not all appear at the same time in the table. If this is the case, you can change the number of devices displayed per page by modifying the value in the **Results by page** box. You can also browse through the different pages, forwards or backwards, using the buttons at the bottom of the table.

In some cases, the number of available parameters is above the number of viewed parameters in the table. You can customize which parameters (columns) are displayed by clicking on the triangle to the right of the heading and checking/unchecking the desired parameters (columns).

You can also sort the table into ascending/descending order by clicking on the column heading you wish to be sorted.

Device dashboards - Widgets

Name	Description	Type of device	Category
CPU	Shows the time evolution for device CPU usage.	All	System
Memory	Shows the time evolution for device RAM usage.	All	System
Storage	Shows the time evolution for flash memory usage.	Router	System
Unresolved critical alarms	List of non-processed critical alarms.	All	System
Unresolved warnings	List of non-processed warnings.	All	System
Throughput (ethernet0/0)	Shows the evolution of the transmission and reception throughput in the indicated interface in bits per second.	Router	System
Throughput	Shows the evolution of the transmission and reception throughput in the indicated radio interface in bits per	Access point	Radio

	second.		
Clients	List of client devices currently connected to the access point.	Access point	Radio
Number of SSIDs	Current number of wireless networks defined for this radio interface	Access point	Radio
RX per client	Shows the evolution of the received bitrate for the selected wireless clients.	Access point	Radio
TX per client	Shows the evolution of the transmitted bitrate for the selected wireless clients.	Access point	Radio
Number of clients	Shows the evolution of the number of wireless LAN client devices connected to this radio interface.	Access point	Radio
Number of rogue clients	Shows the evolution of the number of wireless LAN client devices that have tried to illegally connect to the access point.	Access point	Security
Rogue APs	List of detected, probably illegal, access points. An access point not managed from the platform is considered illegal if it is publishing a wireless network with the same name (SSID) as a network published by one of the managed access points.	Access point	Security
Rogue clients	List of wireless LAN client devices that have tried to illegally connect to the access point. (Secret/keys not known).	Access point	Security
Number of neighbor APs	Shows the evolution, in time, of the number of detected neighbor access points.	Access point	System
Neighbor APs	List of detected neighbor access points.	Access point	System
Neighbor channels	Shows a chart of the radio channels being used by the neighboring access points.	Access point	System
Neighbors signal level	Shows the time evolution for the neighboring access points signal level.	Access point	System
Throughput (Radio #)	Shows the evolution of the transmission and reception throughput for the indicated radio interface in bits per second.	Access point	System
Memory (Physical)	Shows the time evolution of the device's physical memory usage.	Applications host	Global

Memory (Virtual)	Shows the time evolution of the device's virtual memory usage.	Applications host	Global
Memory (Swap)	Shows the time evolution of the device's swap memory usage.	Applications host	Global
HDD	Shows the time evolution of the device's hard disk or USB storage usage.	Application host	Global
HDD (number of files)	Shows the time evolution of the number of files in device storage.	Applications host	Global
CPU	Table showing the CPU usage sharing per application.	Applications host	Global
Memory (Physical)	Table showing the physical memory usage sharing per application.	Applications host	Global
Memory (Virtual)	Table showing the virtual memory usage sharing per application.	Applications host	Global
Memory (Swap)	Table showing the swap memory usage sharing per application.	Applications host	Global
HDD	Table showing the hard drive or USB storage usage sharing per application.	Applications host	Global
HDD (number of files)	Table showing the number of files in the device storage per application.	Applications host	Global
CPU (application)	Shows the time evolution for the CPU usage for a given application.	Applications host	Application
Memory (application)	Shows the time evolution for the memory usage for a given application.	Applications host	Application
HDD (application)	Shows the evolution for the hard disk or USB storage usage for a given application.	Applications host	Application

7.3 How to view detailed information for wireless clients

The ability to monitor the connected client devices and the measured performance for such client devices in terms of tx/rx throughput in a wireless network *is very important*.

The Colibri NetManager platform lets you access the monitoring information for client devices connected to the wireless network in two ways:

- (a) Information on clients connected to one of the wireless networks published on one of the radio interfaces of a given access point.

The monitoring dashboard for an access point shows a table of client devices currently connected to the radio for each radio interface.

You get a table with the following information by clicking on the widget:

- **MAC:** MAC address for the wireless client device connected to an access point.
- **IP:** IP address assigned to the wireless client device.

- **SSID**: name of the wireless network the client is connected to.
- **Status**: state of the client device in terms of connectivity and authentication. The **Status** parameter can be: **Disconnected, Associating, Associated, Authenticating** or **Authenticated**

(b) Information on all client devices currently connected (to any access point).

Select **Dashboard|System|Analysis|Client**. You will see a table showing all the wireless client devices connected to any of the managed access points.

This table contains a search box that allows you to find a device using the device's **MAC** address data. There is also a time filter to search for devices that have had some kind of activity during the specified interval.

In addition to the elements described in the above paragraph (1), the following parameters are displayed for each device:

- **Date**: timestamp of the last exchange with the client device.
- **Throughput**: the last bitrate transmitted and received by the client device.
- **Signal/Noise**: the last signal and noise level (in dBm) values for the client device.
- **Parent**: name of the access point where the client device is connected.
- **Elapsed time**: length of time that the client device has remained in the latest reported state.

7.4 Setting rules for alerts

The Colibri NetManager platform lets you define rules that trigger alerts depending on the values taken by the monitoring parameters in the system.

Select **Dashboard|System|Rules**. A table is shown with the list of currently configured alerts.

To define a rule for generating alerts you should define at least one condition. Complete the following steps:

First, choose the type of device for which you want to define a rule by clicking on the alerts table heading and selecting either **ROUTER, WLAN CONTROLLER, ACCESS POINT** or **CLIENT**.

The next step is to define the trigger condition.

After that, select the alert severity (critical or warning) you wish to define. Then select the parameter to monitor and define the comparison with the desired value or threshold. Once you have defined all the fields click on **Add condition** to add the trigger condition.

If you wish to define additional conditions, please repeat the above. The rule you are defining will only activate if all the conditions are met.

When you have defined all the required conditions click on **New rule** to define and save the rule.

Existing rules can be removed from the system by clicking on **Delete rule** in the row you wish to remove. Please note that once a rule has been deleted, no new alerts associated with this rule are triggered even though the conditions for the deleted rule are met.

You can program the action to be carried out when a rule is triggered, by selecting **Alerts|Actions** and creating new actions.

In order to do this click on **New Action** and define the severity of the alerts that are going to be affected by the action you are defining and the desired report method, email or SNMP trap.

If you select email, enter the email address to which the alerts will be sent in the **Email** box.

If you select SNMP Trap, first select the version of the SNMP protocol to use in the **Protocol version** box. Then enter the IP address or host name of the trap receiver server in the **Trap receiver host** box. Next enter the UDP port number where the trap receiver server is listening in the **Trap receiver port (UDP)** box. Finally, enter the community name to be used for trap sending in the **Community** box.

The parameters that can be used in alerts depend on the type of device. The following list shows the currently supported parameters:

Rules for alerting - Supported parameters

Name	Description	Type of device
CPU	CPU usage.	All except Client
Memory	RAM memory usage.	All except Client
Storage	Flash memory usage.	All except Client
RX	Received throughput (in bps).	Router
TX	Transmitted throughput (in bps).	Router
RX per client	Received throughput by a client (in bps).	Access Point and Client
TX per client	Transmitted throughput by a client (in bps).	Access Point and Client
Number of clients	Number of clients connected to the access point.	Access Point
Noise level	Noise level reported by a client device (in dBm).	Client
Signal level	Signal level reported by a client device (in dBm).	Client

Chapter 8 Device positioning and maps

The Colibri NetManager platform's maps and floor maps are especially suitable for holding large numbers of geographically dispersed operating devices.

The physical location tracking of a device is made easy with powerful graphical and visual element tools allowing you to define the location of each device and place them on a map.

8.1 How to set the device position

There are several ways to establish a device's location in order to place it on a map.

(a) Geo-locating from its public IP address:

Each device connected to the Colibri NetManager platform is automatically assigned a location obtained from its public IP address extracted from the data packets sent by the device. The location is retrieved from a server database holding geo-location data for each public IP address.

The positioning carried out in this way is approximate and the reliability of the locations depends on the accuracy of the public geo-location data published by telecommunication companies.

(b) Establishing the location manually:

The coordinates defining the location of a device can be manually configured by selecting the device from the **Devices** table and clicking on the **Edit** button in the **Details** tab of the device **Info** section.

In the boxes to the right of the **Position** label, enter the latitude in decimal format in the left one and the longitude, also in decimal format, in the right. Next, click on **Save changes** and the device's position is established according to the specified coordinates.

(c) A device with an internal GPS can optionally and periodically send GPS coordinates on its location. In this case the server will place the device at the last position reported by the device.

8.2 How to view devices on a map

You have two choices for viewing a device on a map:

(a) Globally:

If you select **Dashboard|System|Maps**, a map with a default zoom level is displayed so you can see all your devices.






Within the map you can change the position and increase or decrease the zoom level to view the desired area.

Devices located in the same area are shown by a number inside a circle indicating the number of devices in that area. If you are using a mouse, click on the circle and the map adjusts to a zoom level so you can see where all the devices in that area are located.

The following table summarizes the controls available when you are viewing a map:

Maps - Available controls

Icon	Control	Description
	Zoom In	Closes the map around the center.
	Zoom Out	Opens the map around the center.
	Full screen	Changes to full screen mode. Once in this mode press the ESC key to return to

		the normal view.
	Define area	Enters the floor plan editing mode. Please read the next section to learn how to define and configure floor plans.
	Position the device	Manually places a device on the map. When you click on this icon the platform displays a search box to enter the data for the device you wish to position.
	Search device	Search and go to the location of a device. When you click on this icon the platform displays a search box to enter the data of the device you wish to search for.
	My location	Places the map in the current operator location. Your browser may ask you to authorize the use of your location data for privacy reasons.
	Layers	Chooses which layers are shown on the map. There are <i>logical</i> layers with the different types of devices, and <i>physical</i> layers with different levels where several floors with different floor plans have been defined.

(b) For a given device:

Select the desired device from the **Devices** table. Use the **Details** tab to access the device **Info** section and click on the Earth icon to the right of the location coordinates.

To clear the current device coordinates click on the **Clear coordinates** link. You will be asked for confirmation to clear the device coordinates when the window holding the map is closed. Once deleted, the device's coordinates are automatically updated with the IP geo-location data the next time there is contact with the device.

The map controls are the same as described in the previous section.

The **Search device** and **Layers** controls are not available because they are not logical here.

8.3 How to configure floor plans

To setup a floor plan carry out the following steps:

- (1) In map view, select the *Define area* control.
- (2) Click on the vertices in the contour of the polygon area corresponding to the floor plan you wish to define.
- (3) Enter a name for this area in the **Name** box and enter a proper description for this area item in the **Description** box. Then click on **Continue**.
- (4) You can define several floor plans for the same area at different heights or floors. In the next screen enter a name for the floor in the **Name** box and enter the floor level in the **Floor** box.
- (5) If you click on the area tagged as "**Click to upload a map**" you can setup a floor plan for this floor for the area. Files with the floor plans should meet the following requirements:
 - The file format should be JPG, GIF or PNG.
 - They should not exceed 10 megabytes in size.
- (6) Finally click on **Save** to save the floor plan.
- (7) Click on the bullet associated with an area if you wish to modify a previously saved floor plan or add additional floors. A number appears in the bullet indicating how many devices have been placed in this area. Then repeat steps 4 to 6 to define and name additional floors.
- (8) To place a device on a floor plan click on any point of the corresponding area except the bullet. The window containing the map zooms in on the floor plan displaying the image that you previously defined and stored as

the floor plan.

- (9) Click on the *Position the device* control and click where you want the device to be placed and visualized.
- (10) Finally, close the window containing the map. You will be asked for confirmation to permanently store the new device position.
- (11) To change the floor for a device, click on the *Layers* control and choose the desired floor name to change the visualized floor. Then, click on the *Position the device* control to put the device in a new place on the current floor.

Chapter 9 Other management operations

9.1 Processing alerts

If you select the **Alerts** entry from the left-hand menu of the platform, a table with all the pending device alerts is displayed on the central screen.

The **Alerts** table has entries that can remain in *Active* or *Discarded* states.

An active alert is one that has not been processed yet and the cause triggering it remains.

By default only active alerts are shown. The **SHOW ALL** button also shows the discarded alerts.

Alerts also have flags classifying the associated situation as **ERROR**, **WARNING** or **OK**.

The state and flag can be changed by the user when the situation has been diagnosed and solved.

The operator can also choose to add comments on the evolution of the alert by enabling the *Comments* section (by clicking the **Comments** button). Here you can type in explanatory text. You can also click on **Add comment** to include a new comment with this alert.

The number of entered comments for an alert can be seen in a small red balloon at the top right-hand corner of the **Comments** button.

Each row of the **Alert** table holds information on the device originating the alert, the date when the alert was created and modified, the current status and the alert information with a category, name and description.

The alerts can be sorted in different ways (select the sort method in the **Order by** box and click on the arrow to the right) and can be *exported* to a file in CSV format for subsequent analysis.

9.2 Understanding the log section

By selecting the **Devices** menu entry and then clicking on the device you can get a **Log** section listing all the relevant operations carried out from the platform affecting device operation or configuration.

The **Log** table has several log categories. Each category can be selected/unselected by clicking on the corresponding tag in the first row of the table.

Log - Categories

Category	Description
BACKUPS	List of either the configuration backup or data backup operations performed with an Applications host.
RECOVERIES	List of either the configuration restore or data restore operations performed with an Applications host.
COMMANDS	List of special commands sent to a device.
LOGS	List of received logs after issuing a log download operation.
OPERATIONS	List of configuration operations for a device.
TRANSFERS	List of transfer content operations performed by an Applications host.

Each row in the **Log** has two lines. The first describes the log type and the device entity associated with the log entry (System or Application). The second includes a timestamp and the operator (platform user) that launched the operation. If the system (the platform server itself) launched the operation, the user identifier is marked with an **AUTO** label.





To the right of the row an icon appears showing the result of the executed operation.

Log entries can be sorted (by selecting the sorting method in the **Order** box and clicking on the arrow to the right) and *exported* to a CSV file for subsequent analysis.

9.3 Special operations

Various other operations can be launched over the devices in addition to the basic operations of configuring, management and monitoring.

Device - Special Operations

Icon	Operation	Description	Device supported
	Restart	Sends a command telling the device to re-start.	All
	Remove certificates at the device	Sends a command telling the device to remove the certificates and credentials it stored to connect to this server.	All
	Clean cache	Sends a command telling the device to rebuild the installed applications cache. This operation may be required if the device is powered-off while it's installing/uninstalling or upgrading an application.	Application host
	Debug mode	Sends a command telling the device to enter into <i>Debug</i> mode thus increasing the log level.	All
Remove security data	Remove certificates at the server	Removes the credentials stored in the server on the platform. The device should receive a new set of credentials from the server after this operation. This is carried out if the device has a factory default configuration or if you have previously run the <i>Remove certificates from the device</i> operation.	
Request log	Request log	Sends a command telling the device to request the latest log files. Log files can be downloaded from the device Log section.	Application host

9.4 Device firmware upgrade

To upgrade firmware on several devices, select the ones you want from the table using the available filters.

Once you have selected one or more devices, the **Batch operations** button appears in the second row of the device table.

At the **Batch operations** window, select **Load firmware** and click on **Start wizard**.

There are two options for upgrading device firmware using a firmware file:

- If you have a web server with firmware that the device can access, insert the url for the firmware file in the **Enter URL** box.
- If you do not have an external web server, you can upload the firmware file by clicking on the following link: **Upload a file**.

If you have selected several devices, each belonging to a different model, the firmware upgrading screen allows you to specify the models for which the firmware file is valid.

You can also insert several files by clicking on **Add additional file** and assigning each file to the different device models.

The current version only allows you to upgrade the access point firmware.

Click on **Apply** after uploading the firmware file to launch the upgrading process or schedule it by clicking **As soon as possible**, selecting the desired time and clicking Apply.

The firmware upgrading process can be monitored in the device tab, under **Jobs**.

Chapter 10 How Teldat, S.A. licensing works

The licensing model used by Teldat, S.A. depends somewhat on whether you are using, or planning to use, the Colibri NetManager cloud service or whether the platform is installed in your data center.

In both cases, however, you receive a document with a license serial number and a license PIN code when you purchase a license

You need to use this serial number and PIN code for the Colibri NetManager cloud service to activate the license in your subscription.

If the tool is installed in your data center, you can access the Colibri NetManager cloud service to enter the serial number and PIN validation code and retrieve a signed activation file to put on your local tool to activate the license.

10.1 Requesting a new license

Please contact Teldat, S.A. to request a quote for the licenses you require. Once the quote has been received and accepted, you will be sent the license serial numbers and the validation codes. This information should only be entered in the customer environment used to generate the license (customer and servers are defined by a unique value, the UUID).

Teldat, S.A. sells the following licenses:

- **Devices:** These are valid for one year in a cloud server. There is no expiry date for a *Virtual Appliance*.

These licenses are intended to enable devices to be managed from the Colibri NetManager platform. Licenses must be purchased for each device you wish to manage.

- **Applications:** These have no expiry date.

These licenses are intended to enable the installation of an application in an Applications host. There are different licenses and prices depending on the application.

- **Plugins:** These are valid for one year in a cloud server. There is no expiry date for a *Virtual Appliance*.

Plugins are extension modules for the platform itself featuring extra functionalities that are not included by default. Consequently a license is required to activate them.

10.2 Activating a license

Once you have the license serial number and activation code you must register with the Colibri NetManager cloud server to activate a license.

10.2.1 How to activate licenses for the cloud service

- (1) Ingress the cloud service at <https://teldat.networkcloudmanager.com>
- (2) Select **Licenses**.
- (3) Select the cloud service option by clicking on **Manage licenses for this server**.
- (4) Click on **New license**.
- (5) Enter the license serial number in the **Serial Number** box and the PIN validation code in the **License code** box.
- (6) Click on **Register license**.

You have now finished; the new license is automatically activated for the customer requesting the license.

10.2.2 How to activate a license for a virtual appliance installed in your data center

- (1) Ingress the cloud service at <https://teldat.networkcloudmanager.com>
- (2) Select **Licenses**.
- (3) Select a *Virtual Appliance* by clicking on **Manage licenses for local servers**.
- (4) Click on **New license**.
- (5) Enter the license serial number in the **Serial Number** box and the PIN validation code in the **License code** box.
- (6) Click on **Register license**.
- (7) Enter the *Virtual Appliance* customer's UUID (this can be found in the *Licenses* section of your *Virtual Appliance* customer).



Important

The UUID is unique per customer and server. Please enter this information carefully as you will not be able to change it later.

- (8) Download the generated XML file that is only valid for the customer with the UUID used to activate the license and that must subsequently be added to your private Colibri NetManager platform server.
- (9) Ingress your local *Virtual Appliance* and go to the **Licenses** section.
- (10) Click on **New license**.
- (11) Press the **Select file** box and select the XML file that was downloaded in step 8 above. A license file can only be used once; the system will ignore the operation if it is uploaded more than once.
- (12) Click on **Upload license**.

You can access the **Licenses** section in the cloud service via your cloud customer to check the status of your licenses.

Previously generated XML files can also be downloaded again with licenses for your *Virtual Appliance*.

A cloud customer can register both cloud and *Virtual Appliance* licenses.

Please contact us if you have any queries or if you have detected any kind of error when activating your license (such as an invalid UUID).

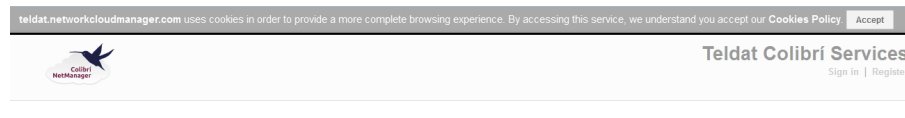
Appendix A Troubleshooting

The following section provides information to help you solve any problems you might encounter during the device registration process and when installing applications. Please contact your distributor if you are unable to resolve a problem.

A.1 Symptom: Cookies message

A cookies message indicating that cookies are blocked appears when accessing the management platform.

Fig. A.1. Cookies blocked on the browser

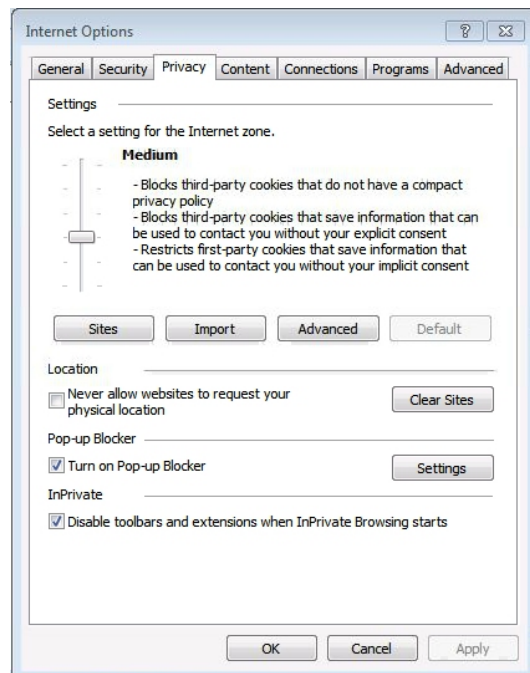


Solution:

To use our website your browser must be configured to accept cookies. We only use one anonymous cookie, which is used to hold a session number. This is only used to maintain the user's session and it neither **references** nor contains any personal or private user information.

For example, if you have Internet Explorer 9, you must first access **Internet Options** from the settings menu and then select the **Privacy** tab and click on the **Advanced** button.

Fig. A.2. Privacy settings



In **Advanced Privacy Settings** select **Override automatic cookies handling** and then select **Accept** in both the **First-party Cookies** section and the **Third-party Cookies** section.

Fig. A.3. Advanced privacy settings

A.2 Symptom: The web site does not work

Solution:

Please make sure that you are using one of the compatible browsers to access our web site. The browsers currently supported are: Internet Explorer 8 or above, Chrome, Firefox and Safari.