

Cloud NetManager Platform

User Guide

Copyright© bintec-DM903-I Version 1.1, 2015 bintec elmeg

Legal Notice

Warranty

This publication is subject to change.

bintec elmeg offers no warranty whatsoever for information contained in this manual.

bintec elmeg 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
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 set up an access point from a configuration template	11
Chapter 5	Monitoring.	13
5.1	Viewing the general system status	13
5.2	Getting the detailed device status	14
5.3	How to view detailed information for wireless clients.	16
5.4	Setting rules for alerts	17
Chapter 6	Device positioning and maps.	19

6.1	How to set the device position	19
6.2	How to view devices on a map	19
6.3	How to configure floor plans	20
Chapter 7	Other management operations.	22
7.1	Processing alerts	22
7.2	Understanding the log section	22
7.3	Special operations	23
7.4	Device firmware upgrade	23
Chapter 8	How bintec elmeg licensing works	25
8.1	Requesting a new license	25
8.2	Activating a license	25
8.2.1	How to activate licenses for the cloud service.	25
8.2.2	How to activate a license for a virtual appliance installed in your data center	26
Appendix A	Troubleshooting.	27
A.1	Symptom: Cookies message	27
A.2	Symptom: The website does not work	28

Chapter 1 About this guide

This is the user guide for the Cloud NetManager platform. The Cloud NetManager platform is a software tool that enables the centralized management of different kinds of network devices.

1.1 Supported devices

The Cloud NetManager platform currently supports the following devices:

The **W1001n**, **W1003n**, **W2003n**, **W2003n-ext**, **W2004n** access points as well as the industrial access point **WI1003n** and the outdoor access points **WO1003n** and **WO2003n**.

1.2 Who should read this manual?

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

1.3 When should I read this manual?

Read this guide once you have registered in the Cloud NetManager platform and received the account activation email. This manual explains how to add devices to the platform. It also details the management operations that can be performed.

1.4 What is in this manual?

This user guide contains the following information:

- An overview of the Cloud NetManager platform software.
- Main concepts and organizational elements of the software.
- How to set up an access point with basic settings.
- How to monitor devices and which parameters that can be controlled.
- 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 on the hardware of devices. While it details the main operations, it is not a comprehensive guide to all management operations available on the platform. This manual does not contain information on how to set up devices for Internet connection. For further information on device configuration, please see the relevant manuals at the following website: <http://www.bintec-elmeg.com>.

1.6 Technical support

bintec elmeg offers a technical support service. Device software can be upgraded on a regular basis for maintenance purposes and for new features.

Contact information:

Web: <http://www.bintec-elmeg.com>

Tel.: +49 - 911 - 9673 0

Fax: +49 - 911 - 688 0725

Email: support@bintec-elmeg.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.

Chapter 2 System overview

2.1 General description

The Cloud NetManager platform is a software tool that enables the centralized management of different kinds of network devices. It can be installed on the existing customer data center infrastructure (*Virtual Appliance*), or be used as a cloud service provided by bintec elmeg

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

The Cloud NetManager platform has configuring and monitoring functions. It also generates reports on incidents and usage while managing the devices.

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

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



A new customer must register at the login screen. Click on **Register**, at the top right corner of the screen, to create 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 set up 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 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.

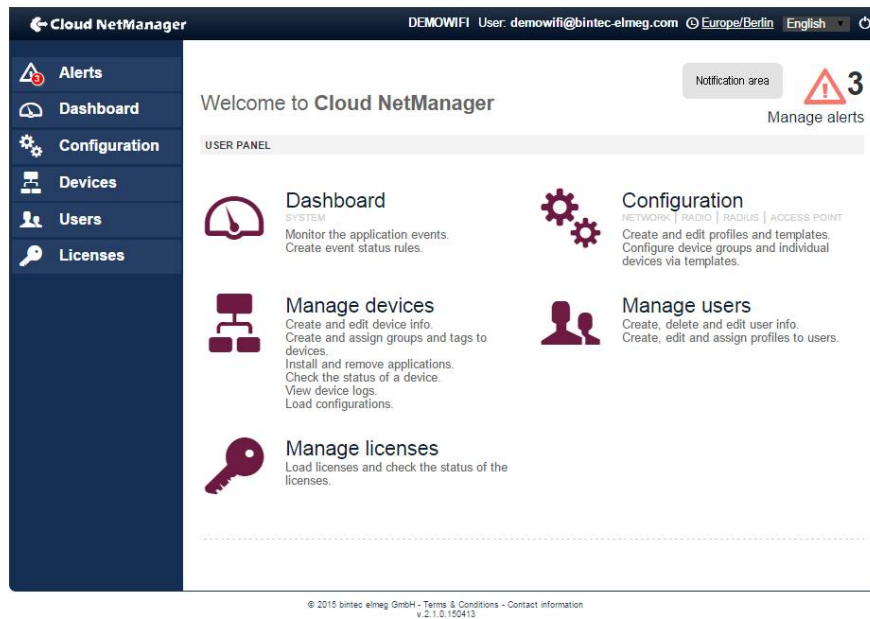
Both SSL server certificates and SSL client certificates are used to establish the connection. This ensures maximum security in data transmission as all messages are encrypted.

Device data traffic does not reach the management platform, meaning the solution is fully scalable.

Users that handle our platform software as a service 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 appears 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 platform entities show how the tool is organized, as well as its management and monitoring operations:

- **Customer:** this entity defines a management environment that can access a given set of devices.
- **User:** this entity features a tool user with a given set of operating permissions (including access to certain devices).
- **Device:** this entity represents the managed network device.
- **Group:** this entity represents a group of devices. A device can only belong to one device group.
- **Tag:** this entity classifies devices. Each device can have a number of associated tags.

3.1 Users and permissions

Users capable of managing and operating current customer devices are defined through the **Users** menu entry.

The user who registers the account (thus becoming the account administrator) must first set up the profiles of any additional users operating 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 relevant boxes.

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

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, including his 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 need to 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, going from fully automatic mechanisms to manual mechanisms for inventoried devices.

Click on **Devices|Add devices** to 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), found on the device label. Using the DVC guarantees 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 on the arrow at the right of each row in the list to access a window with a lock code field. Enter the DVC code and click on 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.



Important

The devices do not need to be connected to the management platform for manual registrations to be performed.

Add devices - Manual registration

Parameter	Description
Mode	Select Enter serial numbers manually for a limited 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 file with comma-separated values and 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 that contains 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.

- **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 the need for an operator (it only requires physical wire connections and for the device to be powered-on and working).

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

The following is an example of option 43:


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

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

bintec elmeg 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. 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 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

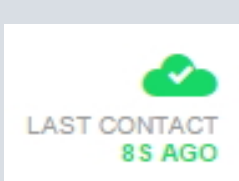
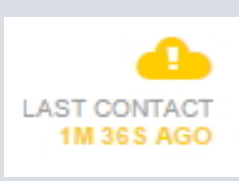
A device must contact the server periodically in order to be managed.

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 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 *Disconnected* state, an alert is raised and pre-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 Cloud 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 where 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 to the devices in the group. You can define a different template for each device type in the group.
Monitoring period	Set up 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. An incorrect use can cause a large number of devices to lose connection to the server and become unmanageable.

- Based on the device, from the Device management section:

Select **Devices** and click on the device you want to create a 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 to classify devices. A device may have multiple **tags** and the same **tag** may be linked to multiple devices.

Tags are primarily used to facilitate the selection of devices for monitoring purposes 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 set up 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 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 wireless devices belonging to the end user.
 - 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** at 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 set up 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 set up an access point, the latter must be included in a group. If you have not created a group yet, 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 following the instructions under paragraph 3 of the previous section.

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

The configuration is applied to the devices for as long as the group parameters and the user operation want.

- 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. 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 **OK** and then **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 to successfully schedule any device configuration updates. When selecting the device, the icon in the notification area must be a green cloud. Otherwise, the device is not reaching the server and the operation cannot be performed.

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

Chapter 5 Monitoring

Device monitoring is one of the most remarkable features of the Cloud NetManager platform.

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

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.

5.1 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 data 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.

5.2 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:

- (a) **Access Point**: Select and view access point devices only.
- (b) **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, located 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 second.	Access point	Radio
Clients	List of client devices cur-	Access point	Radio

	rently connected to the access point.		
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

5.3 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 Cloud 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.

5.4 Setting rules for alerts

The Cloud 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 on the generation of 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 **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 if 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 parameters currently supported:

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 6 Device positioning and maps

The Cloud NetManager platform's maps and floor maps are especially suitable to hold large numbers of geographically dispersed operating devices.

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

6.1 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) Geolocating from its public IP address:

Each device connected to the Cloud 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 geolocation 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 geolocation 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 will be established according to the coordinates specified.

(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.

6.2 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.

A number inside a circle indicates the number of devices in the 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 the 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 geolocation 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 using them here makes little sense.

6.3 How to configure floor plans

To set up a floor plan, carry out the following steps:

- (1) In map view, select the *Define area* control.
- (2) Click on the vertexes 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 "**Click to upload a map**" area, you can set up 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 to indicate how many devices have been placed in this area. 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 select 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 7 Other management operations

7.1 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.

Only active alerts are shown by default. 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 (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 comments entered 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.

7.2 Understanding the log section

By selecting the **Devices** menu entry and then clicking on the device, you can get a **Log** section that lists all the relevant operations that affect the operation or configuration of the device and are carried out from the platform.

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

Log - Categories

Category	Description
BACKUPS	List of the configuration backup or data backup operations performed with an Applications host.
RECOVERIES	List of the configuration restore or data restore operations performed with an Applications host.
COMMANDS	List of special commands sent to a device.
LOGS	List of logs received after launching 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.





An icon appears at the right-hand side of the row 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.

7.3 Special operations

In addition to the basic configuring, management and monitoring operations, several other operations can be launched over the devices.

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

7.4 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. You may also schedule it by clicking on **As soon as possible**, selecting the desired time and clicking on **Apply**.

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

Chapter 8 How bintec elmeg licensing works

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

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

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

If the tool is installed in your data center, you can access the Cloud 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.

8.1 Requesting a new license

Please contact bintec elmeg to request a quote for the licenses you need. 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).

bintec elmeg sells the following licenses:

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

The aim of these licenses is to enable device management from the Cloud NetManager platform. Licenses must be purchased for each device you wish to manage.

8.2 Activating a license

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

8.2.1 How to activate licenses for the cloud service

- (1) Ingress the cloud service at <https://bintec.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.

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

- (1) Ingress the cloud service at <https://bintec.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 XML file generated. Only the customer with the UUID used to activate the license can add it to your private Cloud NetManager platform server.
- (9) Access 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, meaning the system will ignore the operation if the file 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 dealer if you are unable to solve a problem.

A.1 Symptom: Cookies message

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

Fig. A.1. Cookies blocked on the browser

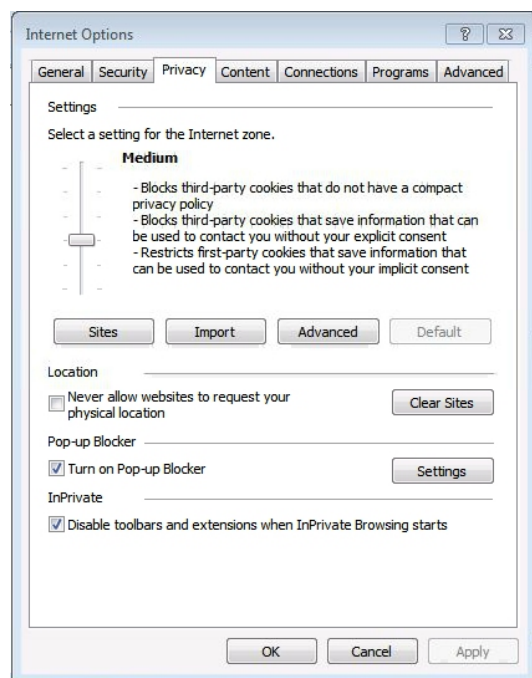


Solution:

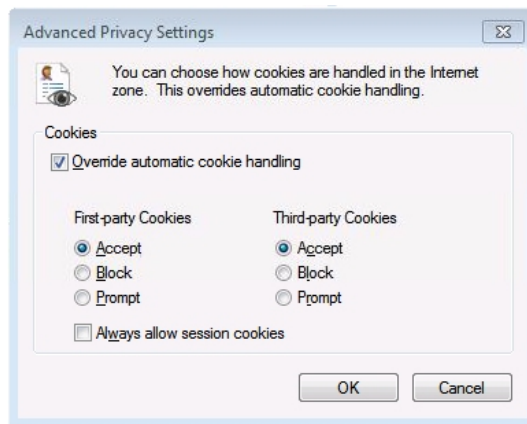
To use our website, your browser must be configured to accept cookies. We only use one anonymous cookie to keep a session number. The goal is to support the user's session, without it referencing or containing any personal or private user information.

For example, if you have Internet Explorer 9, you must first access **Internet Options** at the settings menu, 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 website does not work

Solution:

Please make sure you are accessing our website through one of the compatible browsers. Currently supported browsers are: Internet Explorer 8 or above, Chrome, Firefox and Safari.