Colibri NetManager Platform

Annex: Support to Keymanager feature

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

This is an annex for the Colibri NetManager platform user guide. The Colibri NetManager platform is a software tool designed for managing different kinds of network devices using a centralized approach. This annex explains how configure and manage the Keymanager feature.

1.1 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.

1.2 Related documentation

Dm902-I *Getting started with Colibri NetManager - User's Guide*.

Dm903-I *Colibri NetManager Platform - User's Guide*.

Chapter 2 Configuring routers with the Keymanager feature

To setup a router with the Keymanger feature, first 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 known as parameter *Profiles*. A template defines the whole Keymanager configuration for a device.

The profiles available in a router equipped with a Keymanager feature configuration template are:

- **Configuration|Router Profiles|Security**: Groups all parameters that configure the Keymanager feature (including IP address, a tick indicating whether it is a central server, the Keymanager user and password, and the connections parameters).

  Each connection in the Keymanager feature has the following parameters: central server hostname, preshared key to communicate with the central server, and the means to identify the central server and router (by type).

The next section provides a quick configuration example of a router fitted with the keymanager feature.

> **Important**
>
> On-line help has been added to each parameter belonging to a configuration option and is displayed when you place the mouse over the parameter name.

2.1 Defining a template for a basic router with Keymanager feature setup

To start a router with a configuration template, you must define a security configuration profile.

The steps required to perform a basic configuration are:

(1) Create a security profile:
Select **Configuration|Router Profiles|Security|NEW SECURITY 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 **Device address** box, enter an IP address for the router. This address will be used in IPSec tunnels.
Fill in the **Central server of tunnels** checkbox if the device operates as a central server for IPSec tunnels.
In the **User** box, enter the username needed to access the Keymanager feature.
In the **Password** secret box, enter the password needed to access the Keymanager feature. You can generate a random password by pressing the button to the right of the secret box.
Each connection to an IPSec tunnels central server must be configured via **Connection.**
In the **Central server hostname** box, enter the hostname used to identify the tunnel central server.
In the **Key** secret box, enter a preshared key for IPSec tunnels. You can generate a random password by pressing the button to the right of the secret box.
Specify the central server identity type (e. g., select **IP** in the **Security Central server type of identify** box).
Specify the device identity type (e. g., select **IP** in the **Branch office type of identify** box).
Click on **Save** to finish the security profile.

(2) Create a router configuration template:
Select **Configuration|Device Templates|ROUTER|NEW ROUTER TEMPLATE**. Enter a name for the template in the **Template name** box. This name is used when assigning said configuration template to a group of access points.
To complete the configuration please click on the **Security profile** pull-down menu and select the security profile you created in paragraph 1.
Lastly, click on **Save** to create the new device configuration template.

2.1.1 How to setup a router with the Keymanager feature 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 routers with all the parameters.

To setup a router equipped with the Kermanager feature, the device must be part of a group. If you have not created a group yet, please read Dm903 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 a default configuration template assigned to the group´s access points. To do this, click on the **Configuration Template|Router** menu and select the configuration template created in paragraph 2 of the previous section.

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

The length of time 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 for all the group routes are scheduled and start 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, configuration for the routers is not automatically updated and the operator is responsible for choosing when, and which, devices should be updated.

The operator can choose between a number of different operating procedures when scheduling updates to configure 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 Keymanager feature configuration for the routers 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 where 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 the **As soon as possible** option blank. (this 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 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 reconfigure a single device, first go to the **Devices** section, click on the device row and select the **Configuration** section.

Click on **Security** section to access the Keymanager configuration.

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

⚠ **Important**

Devices must be 'connected' to the server to successfully perform any of the existing procedures for scheduling device configuration updates. When selecting a device, the icon in the notification area must show a green cloud. If said 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 procedure by selecting **Devices**, clicking on the row where the device appears and selecting the **Jobs|Show details** section.