PROSUM

KCenter

Central Management of Distributed IP KVM Extenders

USER'S GUIDE

Version 2.3. December 2017

1 LEGAL NOTICE

1.1 COPYRIGHT 2009-2018 PROSUM

No part of this manual may be reproduced in any form or by any means for other goals that the personal use of purchaser, without written permission from PROSUM.
This handbook cannot be used as a basis of work for the development of any product, documentation, material, and software, without written permission of PROSUM.
PROSUM reserves the right to, without notice, modify all or part of this document and/or make any changes or improvements in any program described in this manual.
PROSUM shall not be liable for any loss, cost, or damage consequential to reliance on this manual.
PROSUM has no liability to the end user or to any third party for consequential damages (including, but not limited to, cost, loss of profits, downtime, damage of equipment or programs).
PROSUM makes no warranty that its software products are error free and will work in combination with any hardware or software products provided by third parties.

1.2 TRADEMARKS AND REGISTERED NAMES

All registered trademarks and registered product names mentioned herein, belong to their respective owners.

2 TABLE OF CONTENTS

3 TABLE OF FIGURES

4 INTRODUCTION

4.1 OVERVIEW

With KCenter, IT administrators can easily manage all Uniclass/Prosum Distributed IP KVMs connected to the LAN or across the Internet. Sets of KMini and/or KLEv2 IP KVM extenders behave like a single distributed, non-blocking multiport IP KVM switch.

Note: In the rest of the document we call "**device**" any one-port IP KVM extender, KMini or KLEv2.

With KCenter, you can:

- Detect and configure all device on your LAN, even when they have wrong IP settings
- See all local and remote device in a dynamic list
- Access to device web management interface with a simple mouse click and without authentication
- Access any computer behind a device by a simple click
- Simultaneously survey and access all computers or a subset of all computers with the Multiviewer
- Backup and restore the configurations
- Update the firmware individually or globally by device model
- Receive all system logs, radius logs, and SNMP traps in a centralized way. All reports are continuously recorded and can be later consulted
- Reboot all or only selected devices

4.2 REQUIREMENTS

4.2.1 KCENTER

KCenter is a java application that can be run on any system with a Java platform installed. The required Java version is 1.7 or higher (Oracle or OpenJDK).

4.2.2 FIREWALL

The following ports must be opened on the computer running KCenter:

- UDP port 80 for device detection.
- UDP port 162 for SNMP trap messages.
- UDP port 1813 for Radius accounting messages. This port number can be modified in the device management.

4.2.3 ROOT SESSION

Linux and MAC OS X Systems: KCenter must be run in a **root** session or with the root privileges.

5 INSTALLING AND RUNNING KCENTER

KCenter has been tested under the following operating systems:

- Windows 10/ Windows 8 /Windows 7 (32 and 64 bits).
- Linux x86 (32 and 64 bits)
- MAC OS X 10.5 or higher.

This chapter describes the installation of KCenter under these systems. Make sure that a Java™ platform is installed on your system before proceeding to the installation. You can download the latest Oracle Java platform from: http://java.com.

You must first proceed to the installation as described below.

5.1 WINDOWS

To install KCenter:

- Run *KCenterSetup.exe* and click *Next* to start the installation
- Select the installation directory, click *Next* and then *Install*

To run KCenter click on the icon located on the computer desktop.

5.2 LINUX

To install KCenter, uncompress the *kcenter_linux.zip* archive. This will create the *kcenter* folder containing *kcenter.jar and multiview-dist.jar*.

To run KCenter,

- The first time, give execution rights to install.sh and run install.sh.
- Then in a terminal change the directory to *kcenter* folder.
  type:
  ```
  $ java -jar kcenter.jar
  ```

5.3 MAC OS X

To install KCenter, open the *kcenter_mac.zip* program. This will create the *installKcenter.pkg* file. Run this program and follow the installation instructions.

To run the program, if just click on the *kcenter.jar* application on the desktop.

6 MAIN PASSWORD

You must login and provide a password to enter into the KCenter application. This password allows you to manage all devices without having to login again to each device.

The default password is **password**.

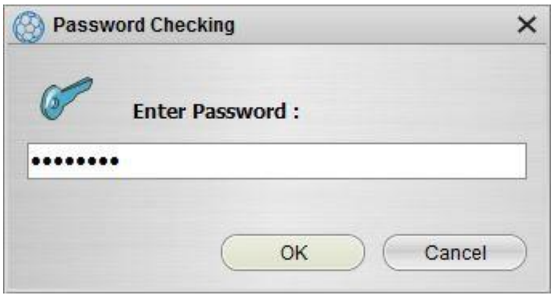


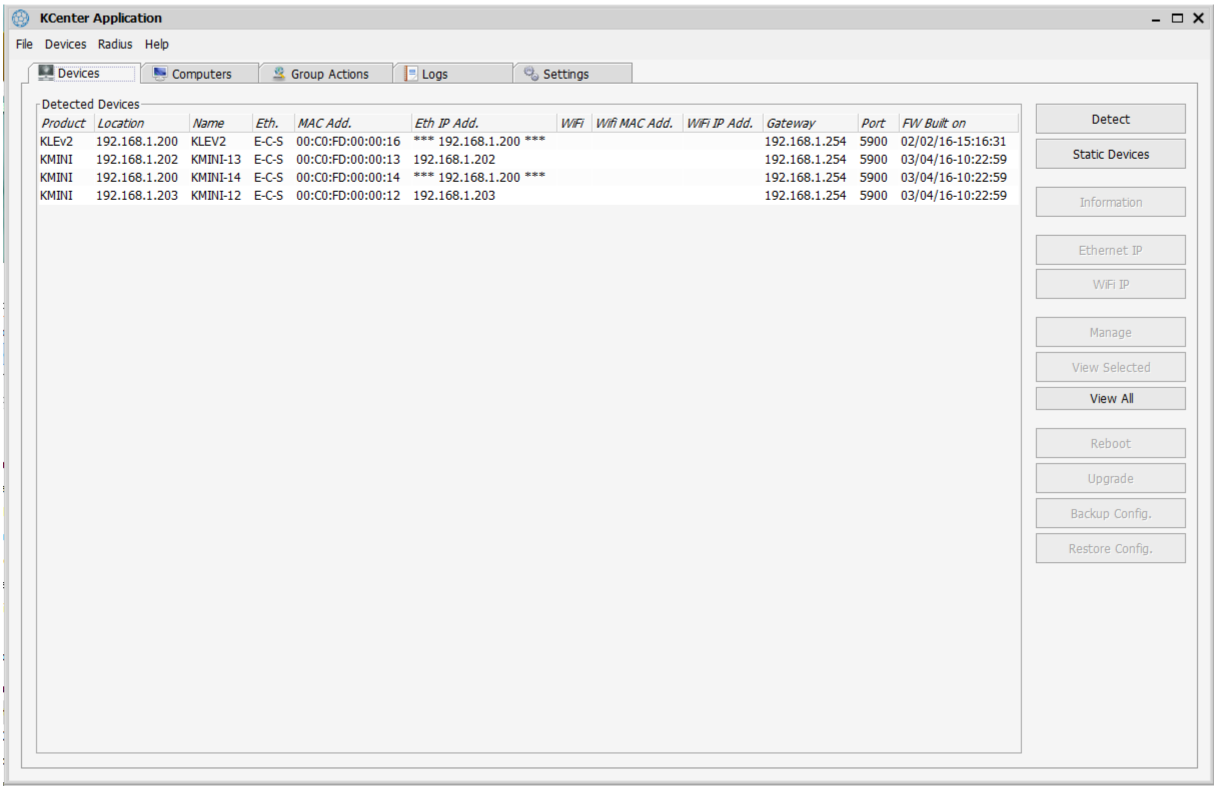
Figure 1 - Main Password Checking Dialog.

Note: It is strongly recommended that you change the password at first application start. To do this, select *Set Main Password* in the *Files* menu.

7 DEVICE PANEL

7.1 DETECTING DEVICES

At start time, KCenter tries to detect all devices and lists them in the panel *Detected Devices*.



Product	Location	Name	Eth.	MAC Add.	Eth IP Add.	WiFi	Wifi MAC Add.	WiFi IP Add.	Gateway	Port	FW Built on
KLEv2	192.168.1.200	KLEV2	E-C-S	00:C0:FD:00:00:16	*** 192.168.1.200 ***				192.168.1.254	5900	02/02/16-15:16:31
KMINI	192.168.1.202	KMINI-13	E-C-S	00:C0:FD:00:00:13	192.168.1.202				192.168.1.254	5900	03/04/16-10:22:59
KMINI	192.168.1.200	KMINI-14	E-C-S	00:C0:FD:00:00:14	*** 192.168.1.200 ***				192.168.1.254	5900	03/04/16-10:22:59
KMINI	192.168.1.203	KMINI-12	E-C-S	00:C0:FD:00:00:12	192.168.1.203				192.168.1.254	5900	03/04/16-10:22:59

Figure 2 – Device Panel

KCenter can detect two types of devices:

- **Dynamic Devices**. They are devices located on your local network. They can be reached directly without using a gateway. These devices are automatically detected by KCenter without needing to specify them.
- **Static Devices**. They are remote devices that cannot be accessed directly but only through a gateway. You must specify their Internet location in order for them to be detected by KCenter.

Note: To detect dynamic devices, KCenter sends a broadcast message on the local network. If some devices are not detected, make sure that your local network permits broadcasting using UDP protocol on port 80. Also make sure that the computer firewall does not block this port for the KCenter application.

Note: The order in which the devices are presented in the list is random. They are added to the list as and when they respond to KCenter scanning. To get a sorted list, click on any column title to sort the Device Panel according to the content of the selected column.

Each line of the device list displays the following information:

Product	Identifies the product type
Location	IP address or host name as detected by KCenter. This field may be different from the IP address of static devices
Name	Device name as configured in the device management
Ethernet	Ethernet interface status. **E**: The interface is Enabled **C**: The interface is connected (Carrier) **S**: IP settings are Static **D**: IP Settings are Dynamic (DHCP)
Ethernet MAC Address	MAC Address of the Ethernet interface
Ethernet IP Address	Ethernet port IP address
WiFi	WiFi interface status **E**: The interface is Enabled **C**: The interface is connected (Carrier) **S**: IP settings are Static **D**: IP Settings are Dynamic (DHCP)
WiFi MAC Address	MAC Address of the WiFi interface
WiFi IP Address	WiFi interface IP address
Gateway	Device default gateway
Port	Base of the range of TCP/IP ports used by device
FW Built on	Date and time of firmware build.

This list is refreshed each time the device detection process is run. It only displays the devices that are currently running.

7.2 MAIN MENU

In the Main menu, click *Devices*. Except *Set Video Compression*, all elements of the *Devices* sub menu have a corresponding button. Refer to the corresponding button in below section *Action Buttons* for a description of the features.

7.2.1 SET VIDEO COMPRESSION

By default, KCenter runs the viewers with fast access options across 10/100 Mbps local area network. However, in the case of static devices located far away on the Internet, the default connection settings may not be appropriate.

You can change the settings to access a specific device by first selecting the device in the list, and then selecting *Devices -> Set Video Compression* in the main menu. The configuration box opens. Select the compression type and the color depth. These settings are saved and will automatically be applied to the device each time you access it. They prevail over the settings saved in the viewer.

7.3 ACTION BUTTONS

The buttons located on the right of the device list allow you to perform set of operations. Buttons *Detect* and *Static Devices* are always enabled because they apply to all devices. The other ones default to grey and are only enabled if they are supported by at least one device that is selected in the list.

7.3.1 DETECT

This button launches the device detection process. By this action, KCenter attempts to discover devices that are located on the local network, and devices that are explicitly specified in the static device list. The device list is updated after the detection process is completed.

Note: You can detect devices:

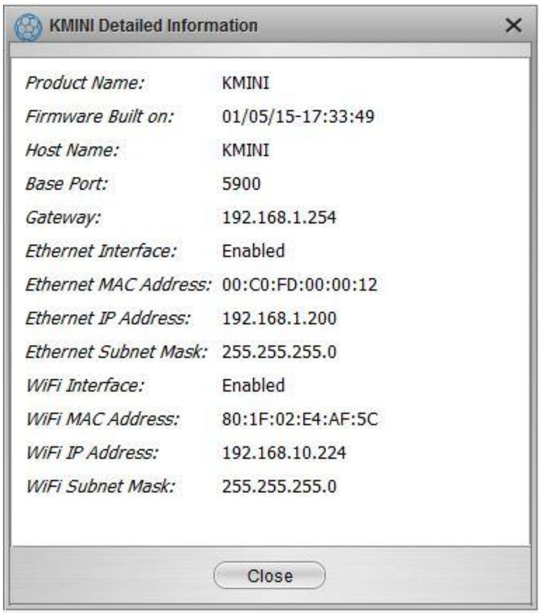
- Manually by clicking *Detect* or by selecting *Detect* in the *Devices* menu
- Manually by double-clicking a device in the list
- Automatically by checking *Detect Devices Periodically* in the *Settings* panel

7.3.2 STATIC DEVICES

This button opens the Static Device Management box.

7.3.3 INFORMATION

This button opens a status box providing device more detailed information about the selected device.

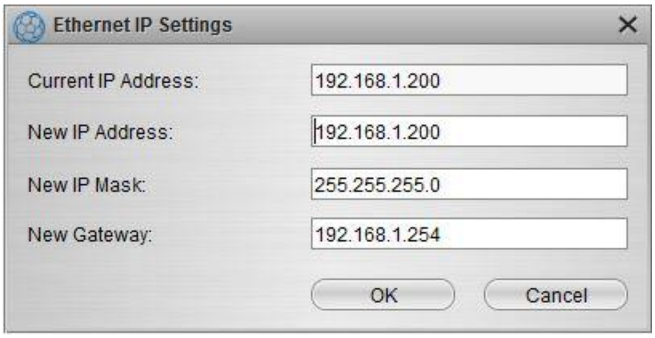


Product Name: KMINI
Firmware Built on: 01/05/15-17:33:49
Host Name: KMINI
Base Port: 5900
Gateway: 192.168.1.254
Ethernet Interface: Enabled
Ethernet MAC Address: 00:C0:FD:00:00:12
Ethernet IP Address: 192.168.1.200
Ethernet Subnet Mask: 255.255.255.0
WiFi Interface: Enabled
WiFi MAC Address: 80:1F:02:E4:AF:5C
WiFi IP Address: 192.168.10.224
WiFi Subnet Mask: 255.255.255.0

Figure 3: Get Device Detailed Information

7.3.4 ETHERNET IP

This button can be used to temporarily modify the device Ethernet interface IP settings. This is only possible if the device is a dynamic device located on your LAN. This action is very useful when the device has been freshly installed on your network, and has not been configured yet. When clicking this button the following dialog box opens:



Current IP Address: 192.168.1.200
New IP Address: 192.168.1.200
New IP Mask: 255.255.255.0
New Gateway: 192.168.1.254

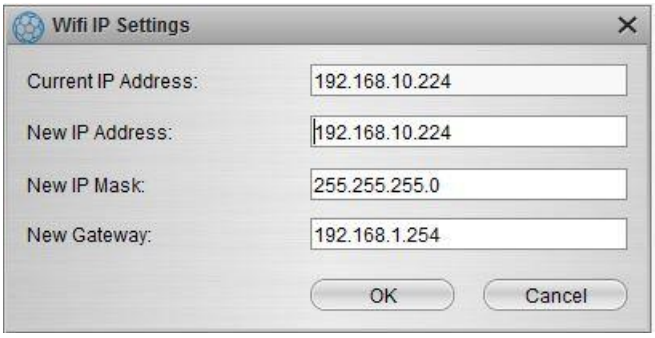
Figure 4: Change Device Ethernet IP Settings

The current IP address is displayed. You can change it, as well as the IP mask and the default gateway. You must fill in these three fields to permit full device access.

Note: All IP settings modified directly by KCenter are only valid until the device reboot. You must run the device management for permanent settings.

7.3.5 WIFI IP

This button can be used to temporarily modify the device WiFi interface IP settings. This is only possible if the device is a dynamic device located on your LAN. When clicking this button the following dialog box opens:



Current IP Address: 192.168.10.224
New IP Address: 192.168.10.224
New IP Mask: 255.255.255.0
New Gateway: 192.168.1.254

Figure 5 - Change Device WiFi IP Settings

The current IP address is displayed. You can change it, as well as the IP mask and the default gateway. You must fill in these three fields to permit full device access.

Note: All IP settings modified directly by KCenter are only valid until the device reboot. You must run the device management for permanent settings.

7.3.6 MANAGE

This buttons launches your current browser so that it automatically tries to access the HTTPS management server of the selected device.

Note: When accessing the device management by this way, the user/password authentication phase is automatically implemented by KCenter. You must setup the credentials in the *Security* tab of the *Settings* panel prior to running this action. See Security Settings.

7.3.7 VIEW

This button launches the viewer that will give you access to the computer attached to the device. This viewer may be the Windows viewer if KCenter is running on a Windows system or the Java viewer if KCenter is installed on Windows, Linux, MAC or another system provided a Java machine is installed. To select the Viewer that will be launched by this button, please go to Device Settings in the *Settings* panel. . You must setup the credentials in the *Security* tab of the *Settings* panel prior to running this action.

7.3.8 VIEW ALL

This button launches the Multiviewer that gives access to all detected devices. The Multiviewer can also show a subset of the devices. Refer to chapter Group Actions Panel. . You must setup the credentials in the *Security* tab of the *Settings* panel prior to running this action.

Note: The arrangement used by the Multiviewer to show the device windows is related to the order in which devices are shown in the Device Panel. By default the order is random. To get a deterministic order, sort the Device Panel by clicking on one of the column titles before clicking this button.

7.3.9 REBOOT

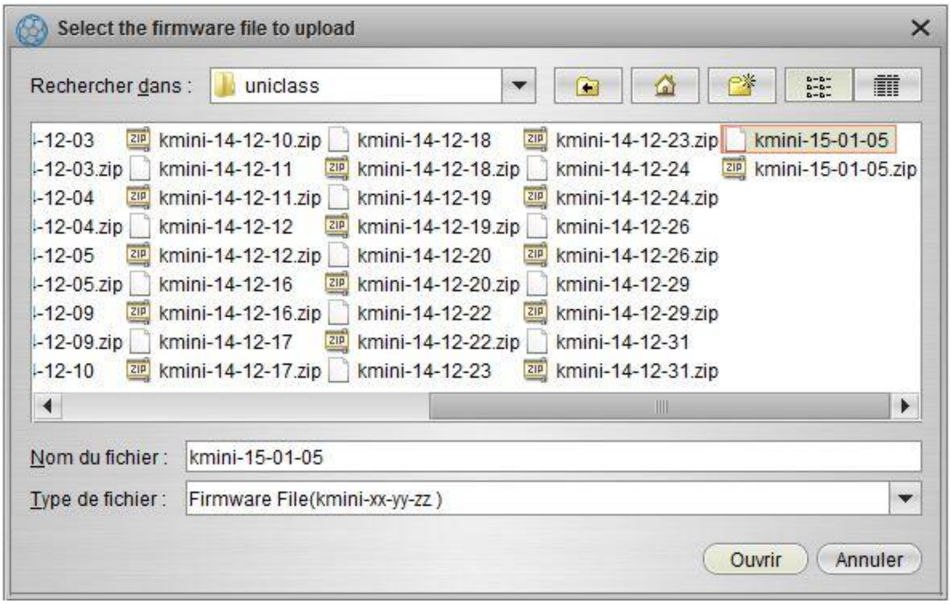
This button allows rebooting the selected device. Following this action, the detection of the rebooted device can take a couple of minutes.

Note: Prior setup of the credentials in the *Security* tab of the *Settings* panel is required.

Note: You can reboot more than one or all the detected devices in the *Group Actions* panel.

7.3.10 UPGRADE

Click this button to upgrade the firmware of the selected device. A dialog box opens, asking you the location of the firmware file:

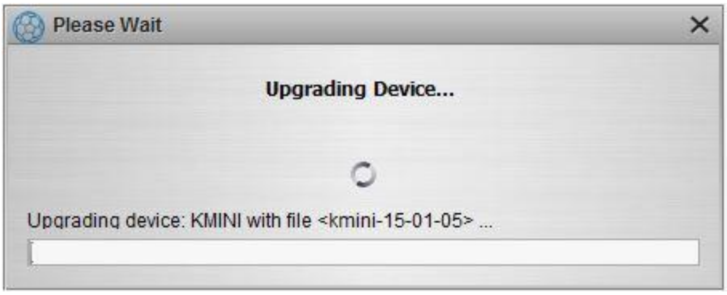


Rechercher dans : uniclass

Nom du fichier : kmini-15-01-05

Type de fichier : Firmware File(kmini-xx-yy-zz)

Figure 6 - Firmware File Selection Dialog



Upgrading device: KMINI with file <kmini-15-01-05> ...

Figure 7: Upgrading Device

Note: You can upgrade more than one or all the detected devices of same type in Group Actions Panel.

7.3.11 BACKUP CONFIG

Click this button to save the configuration of the selected device. A file containing the device configuration is built by KCenter and saved in the folder of your choice. You will be able to restore the saved configuration by clicking the *Restore Config.* button.

Note: Prior setup of the credentials in the *Security* tab of the *Settings* panel is required.

Note: By using the *Group Actions* panel, you can back up the configurations of several or all devices in a single operation.

7.3.12 RESTORE CONFIG

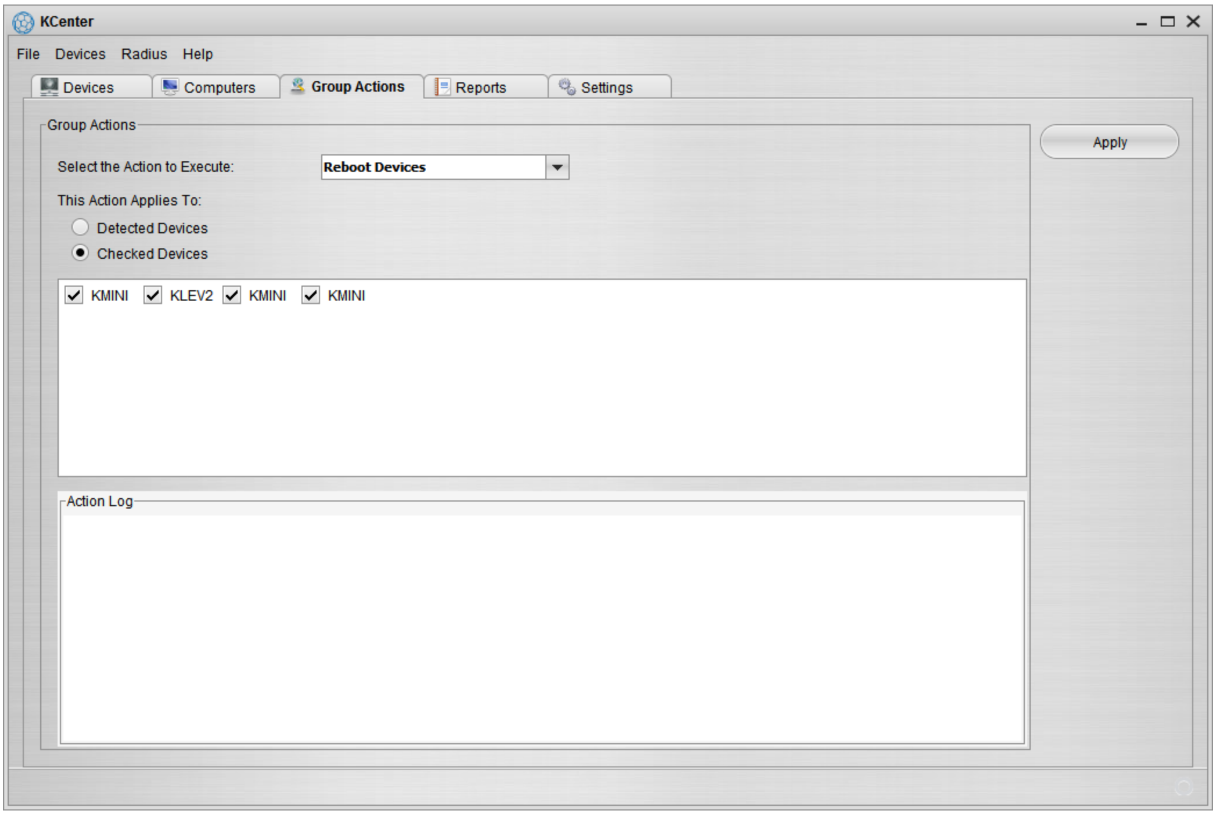
This button allows you to restore a device configuration previously backed up.

Note: Prior setup of the credentials in the *Security* tab of the *Settings* panel is required.

Note: By using the *Group Actions* panel, you can restore the configurations of several or all devices in a single operation.

8 GROUP ACTION PANEL

This panel allows you to apply some actions to more than one device simultaneously. An action can be performed on all devices or on a subset of devices. You can use group actions to reboot devices, upgrade devices, backup and restore device configurations. These group actions are conveyed the same way as single device actions triggered by action buttons (refer to previous section).



Select the Action to Execute: Reboot Devices

This Action Applies To:
○ Detected Devices
● Checked Devices

☑ KMINI ☑ KLEV2 ☑ KMINI ☑ KMINI

Figure 8 - Group Actions Panel

Select the type of action you wish to apply. Select *Detected Devices* or select *Checked Devices* and check the target devices in box. Click *Apply* to perform the action. For each device a message is printed in the *Action Log*. You can check here if the operation has been successful or not.

Note: Prior setup of the credentials in the *Security* tab of the *Settings* panel is required.

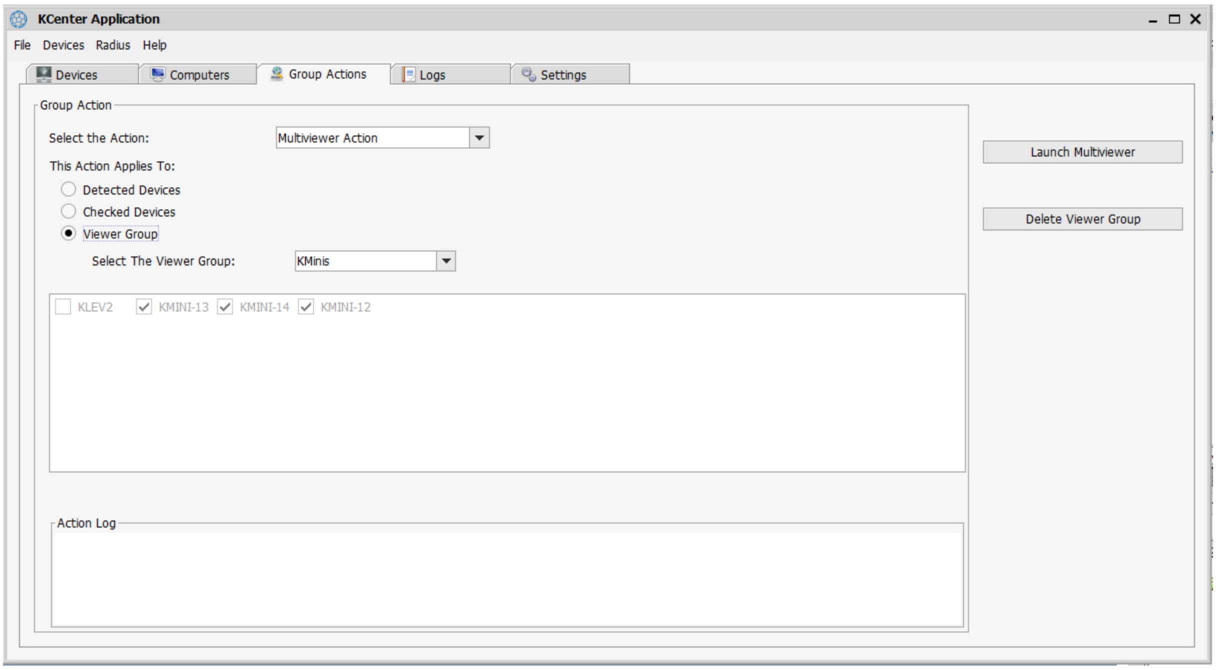
Multiviewer: The Group Action Panel allows running the Multiviewer with more options than the *View All* button of the Device Panel. Select *Multiviewer Action* in the Action List.

To get access to all detected devices with the Multiviewer, check *Detected Devices* and click *Launch Multiviewer*. This is same action as clicking *View All* in the Device Panel.

To access a subset of detected devices, check *Checked Devices* and then check the devices you want to access. Then click *Launch Multiviewer*. You can also save this subset as Multiviewer Group by clicking *Add Viewer Group*. Give a name to the group. The group of checked devices will be saved for future recalls.

To access a Multiviewer Group, check *Viewer Group* and select the group in the list. Then click *Launch Multiviewer*. You can also delete the group by clicking *Delete Viewer Group*. The selected group will be removed from the group list.

There is no limit of the number of Multiviewer Groups. When you display a Group, the devices of the Group will always be shown in same order by the Multiviewer, regardless of the order in which they appear in the Device Panel.



Select the Action: Multiviewer Action

This Action Applies To:
○ Detected Devices
○ Checked Devices
● Viewer Group

Select The Viewer Group: KMinis

☐ KLEV2 ☑ KMINI-13 ☑ KMINI-14 ☑ KMINI-12

Figure 9: Multiviewer Group Action

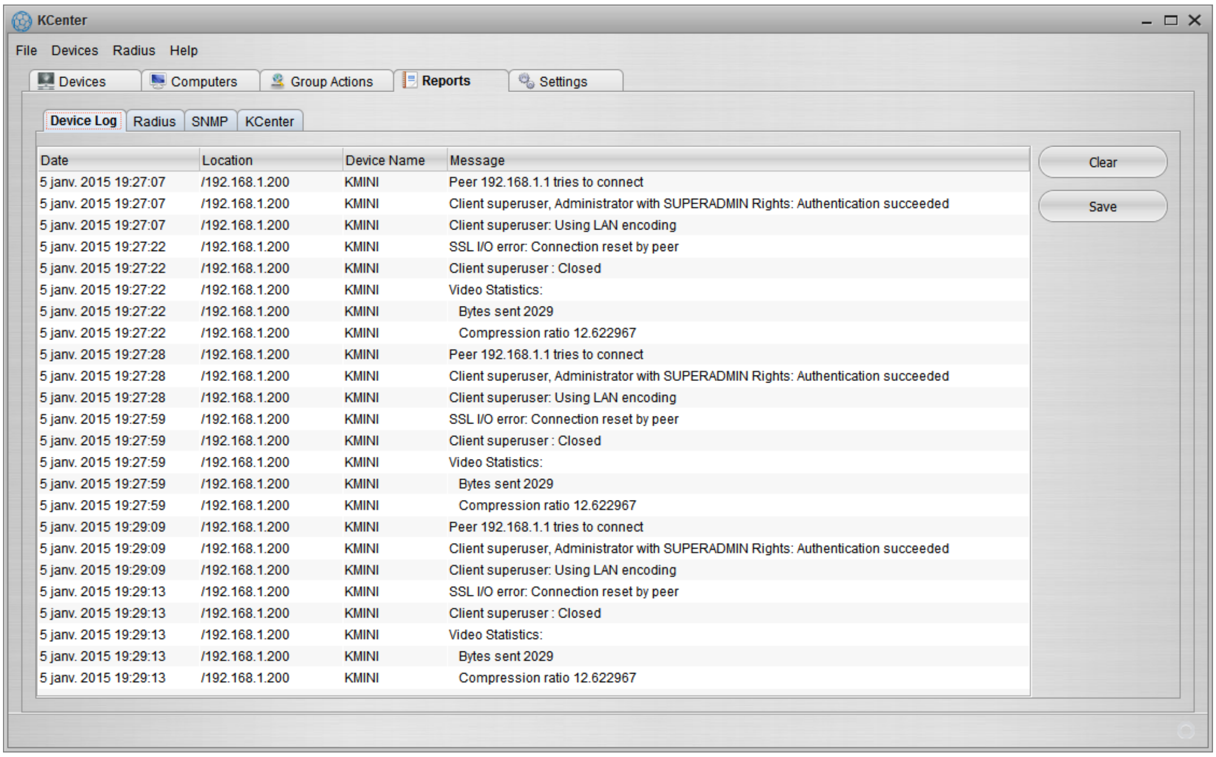
9 REPORT PANEL

Click on *Reports* button to open the Report panel. The Report panel provides four tabs: *Device Log, Radius, SNMP and KCenter*.

Note: In *Log Settings* panel you can set up the number of messages kept in Device, Radius, SNMP, and KCenter logs.

9.1 DEVICE LOG

Click the *Device Log* tab to see the list of all information messages sent by all devices. Prosum IP devices send their information messages automatically to all KCenter applications that contact them. Log messages contain no security sensitive information.



Date	Location	Device Name	Message
5 janv. 2015 19:27:07	/192.168.1.200	KMINI	Peer 192.168.1.1 tries to connect
5 janv. 2015 19:27:07	/192.168.1.200	KMINI	Client superuser, Administrator with SUPERADMIN Rights: Authentication succeeded
5 janv. 2015 19:27:07	/192.168.1.200	KMINI	Client superuser: Using LAN encoding
5 janv. 2015 19:27:22	/192.168.1.200	KMINI	SSL I/O error: Connection reset by peer
5 janv. 2015 19:27:22	/192.168.1.200	KMINI	Client superuser : Closed
5 janv. 2015 19:27:22	/192.168.1.200	KMINI	Video Statistics:
5 janv. 2015 19:27:22	/192.168.1.200	KMINI	Bytes sent 2029
5 janv. 2015 19:27:22	/192.168.1.200	KMINI	Compression ratio 12.622967
5 janv. 2015 19:27:28	/192.168.1.200	KMINI	Peer 192.168.1.1 tries to connect
5 janv. 2015 19:27:28	/192.168.1.200	KMINI	Client superuser, Administrator with SUPERADMIN Rights: Authentication succeeded
5 janv. 2015 19:27:28	/192.168.1.200	KMINI	Client superuser: Using LAN encoding
5 janv. 2015 19:27:59	/192.168.1.200	KMINI	SSL I/O error: Connection reset by peer
5 janv. 2015 19:27:59	/192.168.1.200	KMINI	Client superuser : Closed
5 janv. 2015 19:27:59	/192.168.1.200	KMINI	Video Statistics:
5 janv. 2015 19:27:59	/192.168.1.200	KMINI	Bytes sent 2029
5 janv. 2015 19:27:59	/192.168.1.200	KMINI	Compression ratio 12.622967
5 janv. 2015 19:29:09	/192.168.1.200	KMINI	Peer 192.168.1.1 tries to connect
5 janv. 2015 19:29:09	/192.168.1.200	KMINI	Client superuser, Administrator with SUPERADMIN Rights: Authentication succeeded
5 janv. 2015 19:29:09	/192.168.1.200	KMINI	Client superuser: Using LAN encoding
5 janv. 2015 19:29:13	/192.168.1.200	KMINI	SSL I/O error: Connection reset by peer
5 janv. 2015 19:29:13	/192.168.1.200	KMINI	Client superuser : Closed
5 janv. 2015 19:29:13	/192.168.1.200	KMINI	Video Statistics:
5 janv. 2015 19:29:13	/192.168.1.200	KMINI	Bytes sent 2029
5 janv. 2015 19:29:13	/192.168.1.200	KMINI	Compression ratio 12.622967

Figure 10 – Device Log Tab of Report Panel

Each line of the list shows the following information:

Date	Date and timestamp of message receipt. Note that it may be different from the date and time of the message transmission you can see into the Log page of the device web management
Location	IP address where the message is coming from
Device Name	Source device name
Message	Message content

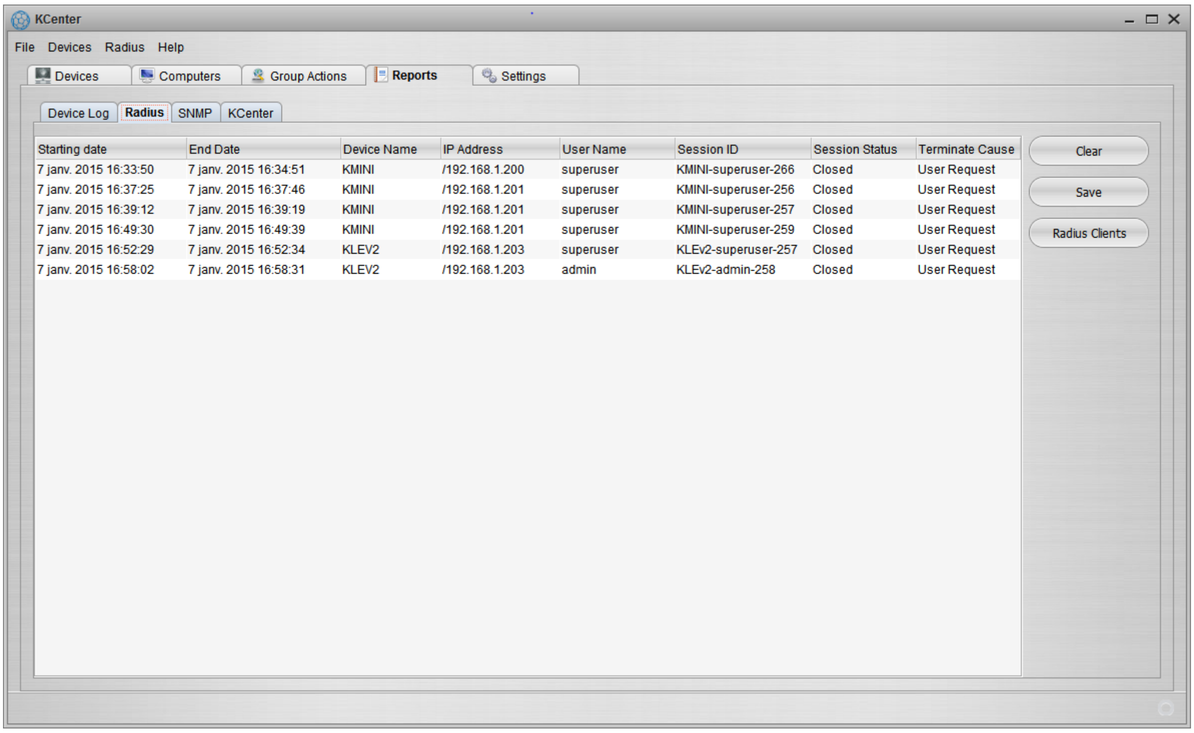
Two buttons are available:

- Clear: clears the log.
- Save: exports the content of the Device log to device.csv located in USER_HOME\.KCenter\Reports\
  - USER_HOME stands for the user's home directory.

9.2 RADIUS ACCOUNTING LOG

KCenter includes a Radius Accounting server able to receive the Radius Accounting messages sent by all devices. The radius accounting shows all client viewer connections and disconnections.

In the Report panel, click the *Radius* tab to see the Radius Accounting messages sent by the devices.



Starting date	End Date	Device Name	IP Address	User Name	Session ID	Session Status	Terminate Cause
7 janv. 2015 16:33:50	7 janv. 2015 16:34:51	KMINI	/192.168.1.200	superuser	KMINI-superuser-266	Closed	User Request
7 janv. 2015 16:37:25	7 janv. 2015 16:37:46	KMINI	/192.168.1.201	superuser	KMINI-superuser-256	Closed	User Request
7 janv. 2015 16:39:12	7 janv. 2015 16:39:19	KMINI	/192.168.1.201	superuser	KMINI-superuser-257	Closed	User Request
7 janv. 2015 16:49:30	7 janv. 2015 16:49:39	KMINI	/192.168.1.201	superuser	KMINI-superuser-259	Closed	User Request
7 janv. 2015 16:52:29	7 janv. 2015 16:52:34	KLEV2	/192.168.1.203	superuser	KLEv2-superuser-257	Closed	User Request
7 janv. 2015 16:58:02	7 janv. 2015 16:58:31	KLEV2	/192.168.1.203	admin	KLEv2-admin-258	Closed	User Request

Figure 11 - Radius Accounting Log

The devices must be set up to send their messages to the IP Address of the computer running KCenter. You must also add all devices either to the *Static Devices List*, or to the *Radius Client List* of KCenter. Note that devices added to the Static Device list are automatically duplicated into the Radius Client list, whereas Dynamic Devices have to be added "manually" to the Radius Client list.

Click on the *Radius* tab to open the log of all Radius Accounting messages sent by IP devices under control. The log is displayed in a list with columns containing the following information:

Starting Date	Date and time of the session starting
End Date	Date and time of the session end
Device Name	Device name as configured in the device management
IP Address	Device IP address as configured in the device management
User Name	Name of the user that makes the session
Session ID	Session identification
Session Status	Current session status
Terminate Cause	Origin of the session end

Note that each session takes a single line. The content of the line is updated when the session is completed.

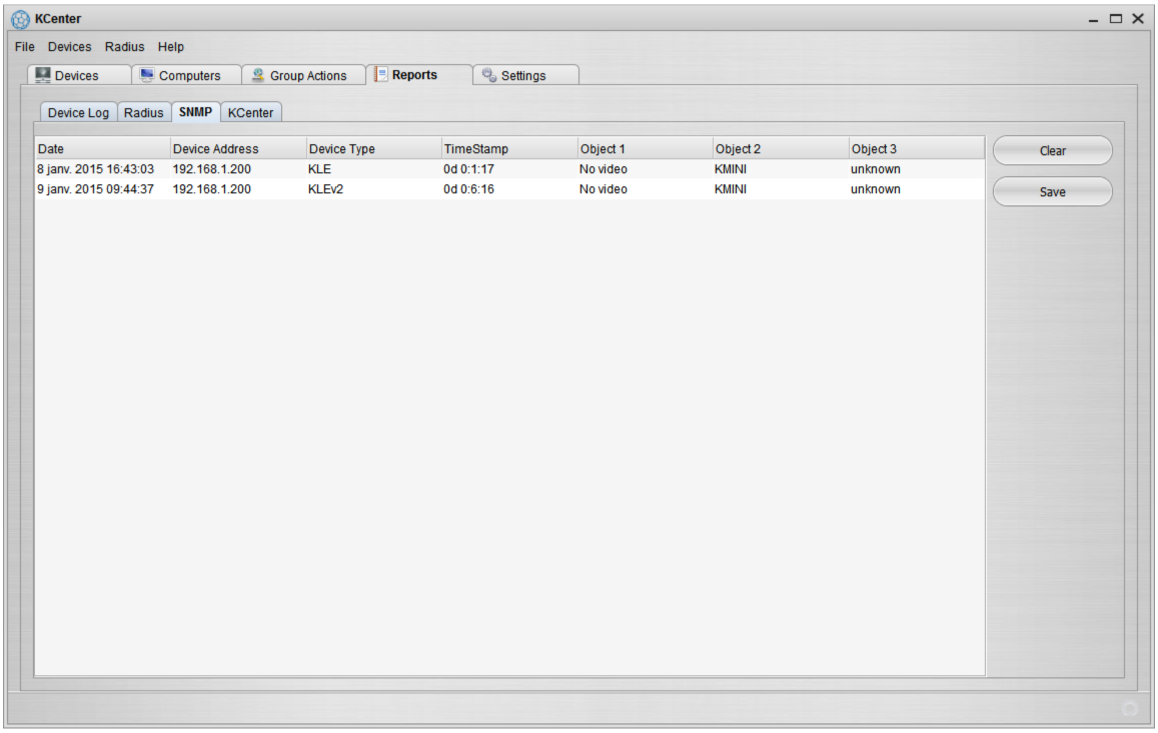
Three buttons are available:

- Clear clears the Radius Accounting log.
- Save exports the Radius Accounting log contents into the radius.csv file located in the "USER_HOME\.KCenter\Reports\" folder - USER_HOME stands for the user's home directory.
- Radius Clients opens the radius client management box. See Radius Client Management.

9.3 SNMP LOG

KCenter can act as an SNMP server receiving alerts (traps) sent by all devices, provided they have been set up to send their SNMP traps to the IP Address of the computer running KCenter.

Click the *SNMP* tab to open the SNMP log.



Date	Device Address	Device Type	TimeStamp	Object 1	Object 2	Object 3
8 janv. 2015 16:43:03	192.168.1.200	KLE	0d 0:1:17	No video	KMINI	unknown
9 janv. 2015 09:44:37	192.168.1.200	KLEv2	0d 0:6:16	No video	KMINI	unknown

Figure 12 - SNMP Log Tab

Each line of the SNMP log contains the following information:

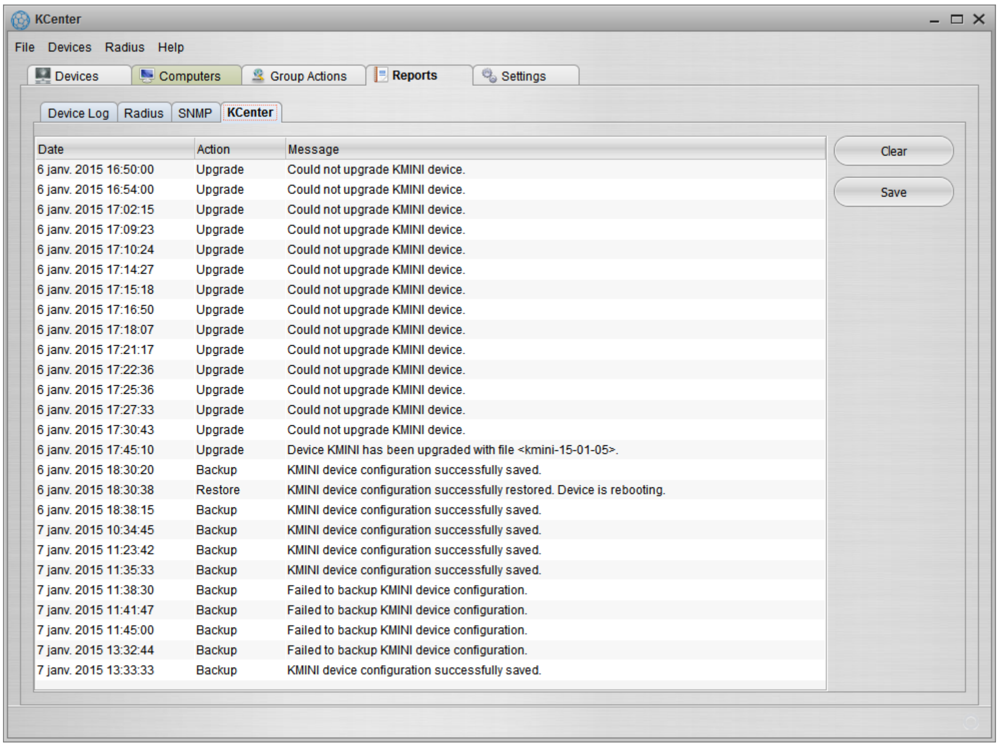
Date	Date and timestamp of the trap
Device Address	Device IP address as configured in the device management
Device Type	Device product type
Time Stamp	Time elapsed since the device has rebooted.
Object 1 Object 2	Trap event as defined in the device SNMP MIB. For more information about objects, consult the device user's manual.

Two buttons are available:

- **Clear** clears the SNMP log.
- **Save** exports the SNMP log contents in to the *snmp.csv* file located in the *"USER_HOME\.KCenter\Reports\"* folder - *USER_HOME* stands for the user's home directory.

9.4 KCENTER LOG

You can see under this tab the messages of KCenter itself.



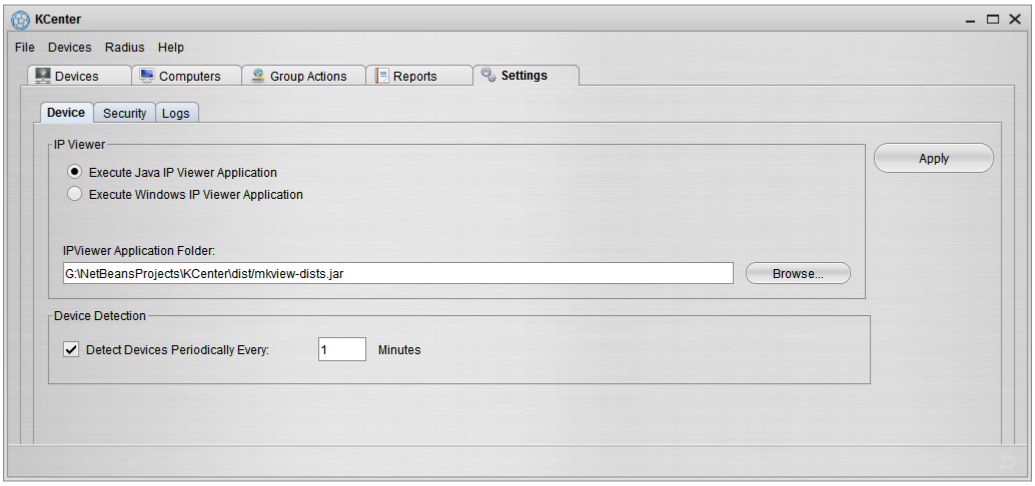
Date	Action	Message
6 janv. 2015 16:50:00	Upgrade	Could not upgrade KMINI device.
6 janv. 2015 16:54:00	Upgrade	Could not upgrade KMINI device.
6 janv. 2015 17:02:15	Upgrade	Could not upgrade KMINI device.
6 janv. 2015 17:09:23	Upgrade	Could not upgrade KMINI device.
6 janv. 2015 17:10:24	Upgrade	Could not upgrade KMINI device.
6 janv. 2015 17:14:27	Upgrade	Could not upgrade KMINI device.
6 janv. 2015 17:15:18	Upgrade	Could not upgrade KMINI device.
6 janv. 2015 17:16:50	Upgrade	Could not upgrade KMINI device.
6 janv. 2015 17:18:07	Upgrade	Could not upgrade KMINI device.
6 janv. 2015 17:21:17	Upgrade	Could not upgrade KMINI device.
6 janv. 2015 17:22:36	Upgrade	Could not upgrade KMINI device.
6 janv. 2015 17:25:36	Upgrade	Could not upgrade KMINI device.
6 janv. 2015 17:27:33	Upgrade	Could not upgrade KMINI device.
6 janv. 2015 17:30:43	Upgrade	Could not upgrade KMINI device.
6 janv. 2015 17:45:10	Upgrade	Device KMINI has been upgraded with file <kmini-15-01-05>.
6 janv. 2015 18:30:20	Backup	KMINI device configuration successfully saved.
6 janv. 2015 18:30:38	Restore	KMINI device configuration successfully restored. Device is rebooting.
6 janv. 2015 18:38:15	Backup	KMINI device configuration successfully saved.
7 janv. 2015 10:34:45	Backup	KMINI device configuration successfully saved.
7 janv. 2015 11:23:42	Backup	KMINI device configuration successfully saved.
7 janv. 2015 11:35:33	Backup	KMINI device configuration successfully saved.
7 janv. 2015 11:38:30	Backup	Failed to backup KMINI device configuration.
7 janv. 2015 11:41:47	Backup	Failed to backup KMINI device configuration.
7 janv. 2015 11:45:00	Backup	Failed to backup KMINI device configuration.
7 janv. 2015 13:32:44	Backup	Failed to backup KMINI device configuration.
7 janv. 2015 13:33:33	Backup	KMINI device configuration successfully saved.

Figure 13: KCenter Log

10 SETTINGS PANEL

The *Settings* panel is the place where you can configure KCenter according to your wishes, environment, and IP Devices. It contains three tabs, the first one for Device settings, the second one for Security settings and the last one for Log settings.

10.1 DEVICE SETTINGS



IP Viewer

● Execute Java IP Viewer Application

○ Execute Windows IP Viewer Application

IPViewer Application Folder: G:\NetBeansProjects\KCenter\dist/mkview-dists.jar

Device Detection

☑ Detect Devices Periodically Every: 1 Minutes

Figure 14 - Device Setting Panel

10.1.1 IP VIEWER

If KCenter is installed on a **Windows** system, you can select the application that is run when you click on the *Viewer* button for IP KVM devices. Select either *Execute Java IP Viewer Application* or *Execute Windows IP Viewer Application.* You must ensure that the viewer application is installed and you must specify the complete application path. Click *Apply* to validate your modifications.

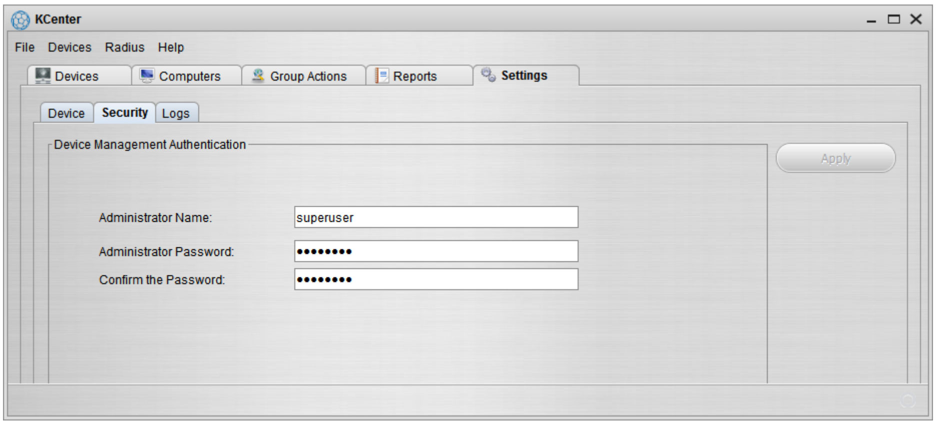
If KCenter is installed on a **Linux or Mac OS X system**, only the second option is available since only Java viewers can be run under these systems. You must specify a valid path for the java viewer - package with jar extension.

10.1.2 DEVICE DETECTION

By default the device detection is run at start time or manually by clicking on the *Detect* button of the *Devices* panel. By checking *Detect Devices Periodically,* the device detection will run periodically. Fill in the period in minutes.

10.2 SECURITY SETTINGS

In *Security* panel you must setup the credentials that will be used by KCenter to access ALL devices.



Administrator Name: superuser

Administrator Password: ••••••••

Confirm the Password: ••••••••

Figure 15 - Security Settings

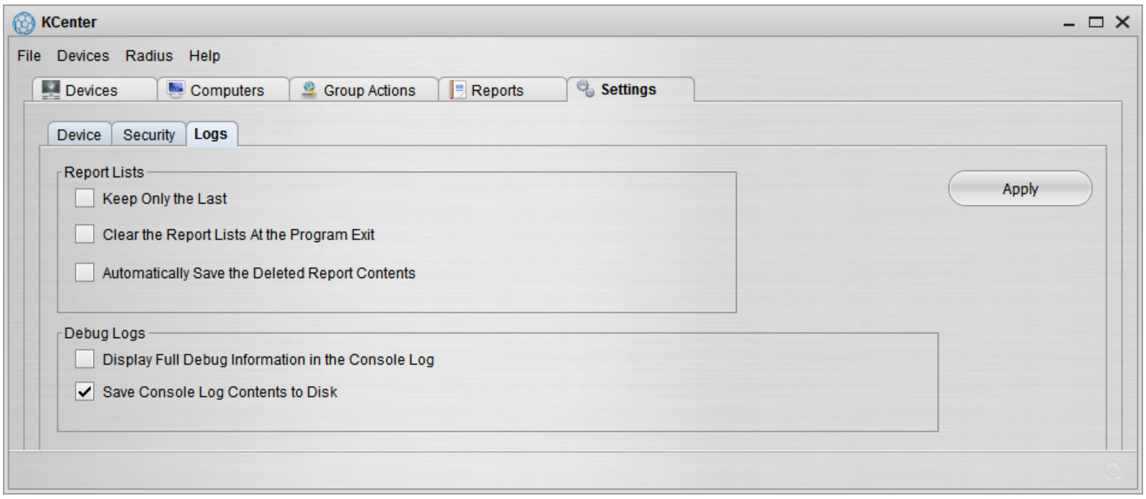
All devices that KCenter must be able to access must have one super-administrator user corresponding to these credentials.

For example in all devices add a super administrator user "kcenter" with password "kcenterpass". Then fill in *Administrator Name* with "kcenter" and *Administrator Password* with "kcenterpass". Confirm the password and click *Apply* to validate your modifications. Starting from now KCenter will access the devices as user "kcenter/kcenterpass".

Note: Preferably use a complex password with a mixture of uppercase letters, lowercase letters, and numbers. After everything have been set up you will not have to type it anymore.

10.3 LOG SETTINGS

Use this panel to set up the options related to report lists and program debug messages.



Report Lists
☐ Keep Only the Last
☐ Clear the Report Lists At the Program Exit
☐ Automatically Save the Deleted Report Contents

Debug Logs
☐ Display Full Debug Information in the Console Log
☑ Save Console Log Contents to Disk

Figure 16: Log Settings

10.3.1 REPORT SETTINGS

The following options are available for the report lists:

- *Keep Only the Most Recent:* When this box is checked, you can set up the number of most recent messages that will be displayed in the report lists
- *Clear the Report Lists at Program Exit:* When this box is checked, all report lists are cleared when the program terminates. Otherwise, the lists are kept and restored at next start
- *Automatically Save the Deleted Report Contents:* Permits to save the messages that are deleted because at least one of the two previous boxes is checked. Refer to section *Report Panel* to know the file name of report lists. Note that the lists cleared by clicking the *Clear* buttons are not concerned by this option

10.3.2 DEBUG LOGS

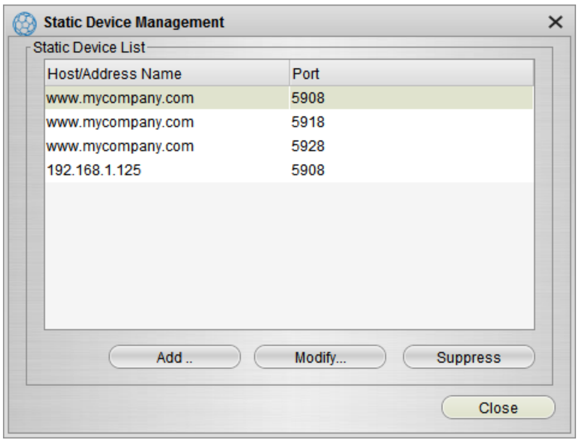
By default, KCenter program sends messages resulting from unattended events to the Java console. You can control the types and destination of these messages by checking the following boxes.

- *Display Full Debug Information in the Console Log:* When this checkbox is set, KCenter will send more detailed information to the Java console
- *Redirect Console Log Contents to Disk:* Specifies that debug messages are not sent to the Java console but saved in files located in the “USER_HOME\.KCenter \Debug” folder

Note: You should not check these boxes unless you are asked to do so by the technical support of Prosum.

11 STATIC DEVICE MANAGEMENT

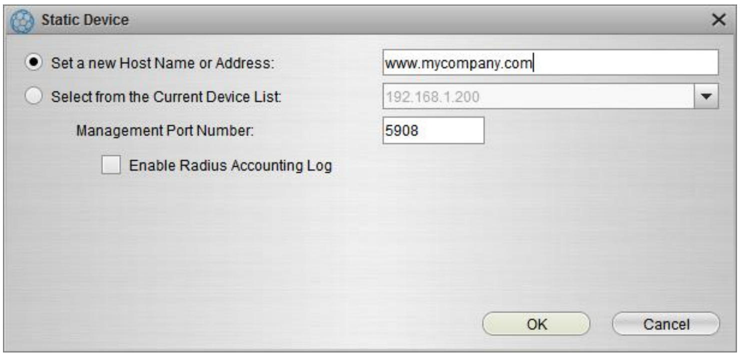
You can manage static devices by clicking on the *Static Devices* button in the *Devices* panel or in the *Devices* menu. It opens a box showing the list of configured static devices:



Host/Address Name	Port
www.mycompany.com	5908
www.mycompany.com	5918
www.mycompany.com	5928
192.168.1.125	5908

Figure 17 - Static Device Management

In this dialog box you can add a new static device, modify, or suppress an existing device. When clicking on *Add ...* or *Modify...* buttons, the following dialog box opens:



● Set a new Host Name or Address: www.mycompany.com
○ Select from the Current Device List: 192.168.1.200
Management Port Number: 5908
☐ Enable Radius Accounting Log

Figure 18 - Static Device Edit

You can specify a static device by entering its host name or dot-decimal IP address.

Note: In case of remote device, located over the Internet for example, take care to specify a public IP address or host name (i.e. the Internet address) and not the LAN IP address set up in the device web management.

Note: You can transform a Dynamic Device into Static Device by entering its LAN IP address, or simply by selecting it in the device list.

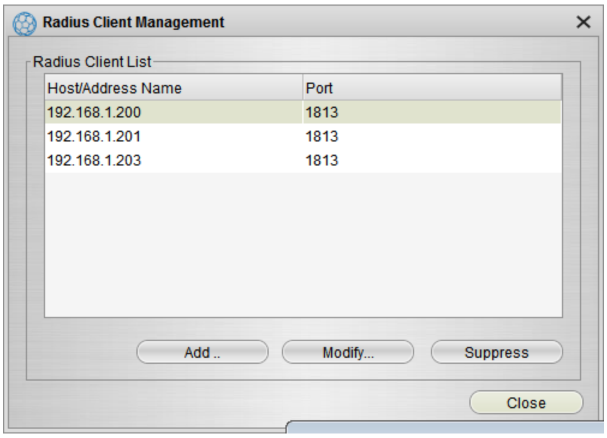
If you want to receive centralized reports for radius accounting logs, check the *Enable Radius Accounting Log* box. Enter the *Radius Port* number and the *Radius Secret* as configured in the specific device management.

Note: When you check the *Enable Radius Accounting Log* selection, the device is automatically added to the Radius Client list. Refer to the following section.

12 RADIUS CLIENTS

To receive *Radius Accounting* logs from devices, you must specify device specific Radius information in the *Radius Client* management. You can access to Radius Client management by selecting *Radius Clients* ... in the *Radius* menu, or by clicking on the *Radius Clients* button in the *Radius Log* view. See Reports Panel.

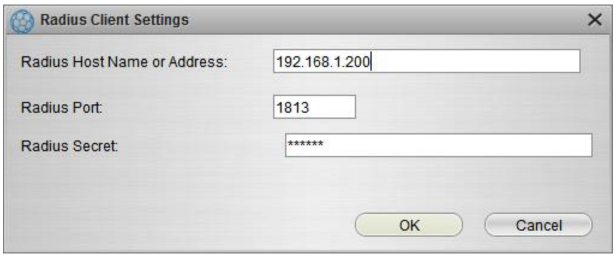
You can also configure new or old radius clients in the Static Device Management. The list of IP addresses and ports of client devices set up for *Radius Accounting* is displayed.



Host/Address Name	Port
192.168.1.200	1813
192.168.1.201	1813
192.168.1.203	1813

Figure 19: Management of Radius Client List

To modify or add new clients to the list, click the corresponding button.



Radius Host Name or Address: 192.168.1.200

Radius Port: 1813

Radius Secret: ******

Figure 20: Radius Client Settings

Radius Host Name or Address	Enter the device host name or its IP address
Radius Port	Port used by Radius accounting protocol to send UDP messages
Radius Secret	Shared secret used by Radius Accounting client to send messages. By default, you enter it in password format. To see it in clear, check *Show Secret* – available only at first creation time

13 MULTIVIEWER

The Multiviewer is able to give a KVM access to several devices simultaneously. The Multiviewer is installed with KCenter. It is a companion application that cannot be run alone. It is launched by KCenter and it gives access to all detected devices or to a subset of the devices according to the settings you made in KCenter (See Devices and Group Actions).

13.1 ARRANGEMENT OF INTERNAL WINDOWS

At start time the screens of all devices are automatically arranged in small windows on a grid basis and scaled so that they can all fit into the Multiviewer main window.

The order of internal windows is dictated by the order of devices in the device-list of KCenter. To get an order that is not random, sort the KCenter device-list before launching the Multiviewer.

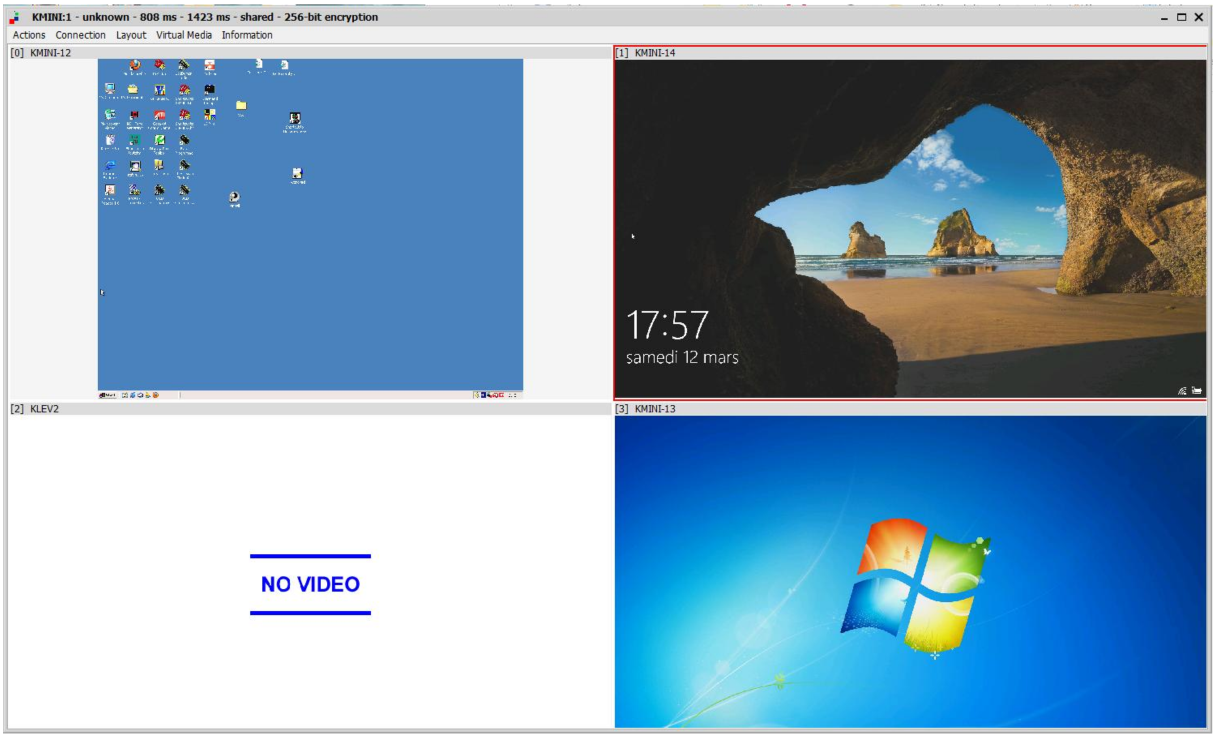


Figure 21: Multiviewer

13.2 MULTI -VIEW AND SINGLE-VIEW

The Multiviewer can switch between the multi-view display and a single-view display of one of the devices at normal resolution. The switching is fast. You can toggle between the multi-view and the single-view displays by **clicking on a device window while pressing CTRL/SHIFT**.

Single-view mode: the Multiviewer behaves like a standard KVM viewer. The video is displayed at normal resolution without scaling.

Multi-view mode: the Multiviewer shows several devices, however the mouse and keyboards are responsive. The mouse and keyboard events are sent to the device under the mouse cursor.

13.3 SELECTED DEVICE

The **selected device** is highlighted by red borders. To select a device just click in its window. The selected device has its information displayed in the Multiviewer system bar. The menu bar *Action* and *Connection* sub-menus apply to the selected device.

13.4 LAYOUT OF INTERNAL WINDOWS

The layout of windows is flexible. At start time the Multiviewer arranges the windows on a grid layout depending on the number of devices. Then **the windows can be dragged or resized** provided the option *Move and Resize Windows* is checked in the *Layout* sub-menu.

A **custom layout** can be saved and reused later.

The layout can be elastic or not. When the elastic layout is enabled, all windows are automatically resized when you modify the size of the Multiviewer main window. When the layout is not elastic, the internal windows are not modified, allowing for example to increase the main window to create space for a custom layout.

13.5 WINDOWS DECORATION

The internal device windows can be naked or decorated with a label showing the device name or the device IP address (Location). This feature can be set up in the *Layout* sub-menu with the *Decorated Windows* and *Show IP addresses* check boxes.

Double clicking on the decoration label makes the Multiviewer open the web management of the device

13.6 DIFFERENCES WITH THE STANDARD VIEWERS

The Multiviewer

- must be launched by KCenter,
- gives simultaneous access to a subset or to all devices,
- saves the hassle of typing the user/password for each device,
- automatically reconnects the devices that have lost their connection,
- shows a message in the windows of devices that are out of reach,
- allows to modify the connection settings on the fly for each device and automatically records them for future sessions with this device,
- automatically scale the video of devices,
- can launch the management of a device,
- has some different menu commands.