PRIMA Center

Centralized Management Solution for
PROKLE, PRIMA-IP, and ioPower.net Devices

USER'S GUIDE

Version 1.1
March 2012

LEGAL NOTICE

1.1 COPYRIGHT 2009-2012 PROSUM

1.2 TRADEMARKS AND REGISTERED NAMES

TABLE OF CONTENTS

TABLE OF FIGURES

1 INTRODUCTION

1.1 OVERVIEW

With PRIMA Center, IT administrators can easily manage all Prosum IP products connected to the LAN or across the Internet such as IP KVM Switches, Power Control devices, Digital Signage devices etc...

With PRIMA Center, you can:

- Detect and configure all devices on your LAN, even when they have wrong IP settings
- See all local and remote devices in a dynamic list
- Access to device web management interface with a simple mouse click and without authentication
- Launch automatically the correct viewers or management applications depending on the device model
- 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

1.2 REQUIREMENTS

1.2.1 PRIMA CENTER

PRIMA Center is a java application that can be run on any system with a Java platform installed. The required Java version is 1.6.0.23 or higher (Oracle or OpenJDK).

1.2.2 FIREWALL

The following ports must be opened on the computer running PRIMA Center:

- 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.

1.2.3 ROOT SESSION

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

1.2.4 FIRMWARE VERSION

All IP products under management must have a firmware recent enough to support PRIMA Center management. If necessary, upgrade the concerned devices with the latest firmware version.

2 INSTALLING AND RUNNING PRIMA CENTER

PRIMA Center has been tested under the following operating systems:

- Windows 7 (32 and 64 bits)/Vista/Server 2008/XP/Server 2003.
- Linux x86 (32 and 64 bits)
- MAC OS X 10.5 or higher.

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

You must first proceed to the installation as described below. Then, if you already registered PRIMA Center, insert the USB key dongle into a USB port of the computer.

2.1 WINDOWS

To install PRIMA Center:

- Run *PRIMA CenterSetup.exe* and click *Next* to start the installation
- Select the installation directory, click *Next* and then *Install*
- At the completing Wizard screen, check *Install Windows USB Key Driver* and click *Finish*.
- If a security dialog box asks you to install the *Keylok Usbkey* driver, click *Install*

To run PRIMA Center click on the icon located on the computer desktop.

2.2 LINUX

To install PRIMA Center, uncompress the *primacenter_linux.zip* archive. This will create the *primacenter* folder containing *primacenter.jar*. Please note that PRIMA Center can only run with the root privileges.

To run PRIMA Center,

- The first time, give execution rights to install.sh and run install.sh.
- Then in a terminal change the directory to *primacenter* folder.
  If you are root, type: `# java –jar primacenter.jar`
  Otherwise type: `$ sudo java –jar primacenter.jar`

2.3 MAC OS X

To install PRIMA Center, open the *primacenter_mac.zip* program. This will create the *installPrimacenter.pkg* file. Run this program and follow the installation instructions.

To run the program, if you are the root, just click on the *primacenter.jar* application on the desktop. PRIMA Center will run. If you are not in a root session, open a console into */Applications/Primacenter* folder, and type: `$ sudo java –jar primacenter.jar`

3 LICENSING SCHEME

3.1 LICENSE AND USB KEY

To run PRIMA Center you must obtain a user license file. This license file controls the number of devices that PRIMA Center can manage. We deliver trial licenses that permit to evaluate PRIMA Center for a limited time without USB key.

When registering PRIMA Center, you are delivered a USB key that unblocks the program beyond the trial period, and a license file corresponding to the number of supported devices you purchased.

The first time PRIMA Center is run, it requests a license file. (See Figure 1)

Figure 1 - License Validating Dialog.

Unless this is a trial license, insert your USB key in a USB port of the computer and enter the complete license file path. Click *OK* to validate. Once the license file has been found and validated, the license information is displayed in the main frame:

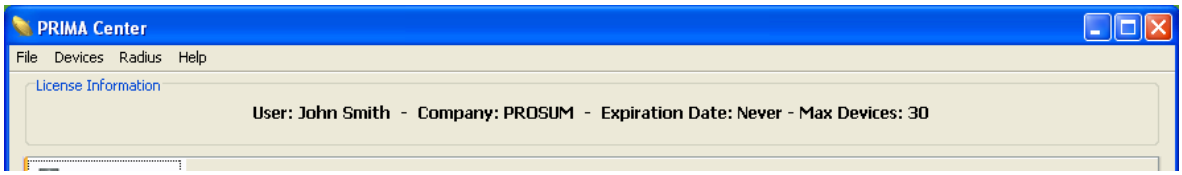

Figure 2 - License Information as Displayed in the Main Frame.

The license information contains the user and company names, the expiration date in case of a trial license, and the maximum number of devices that can be managed.

Note: You can purchase extra licenses to extend the number of managed devices. Refer to following section.

3.2 LICENSE MANAGEMENT

To open the license management box, select *Manage Licenses…* in the *Help* menu. It shows the list of licenses installed.

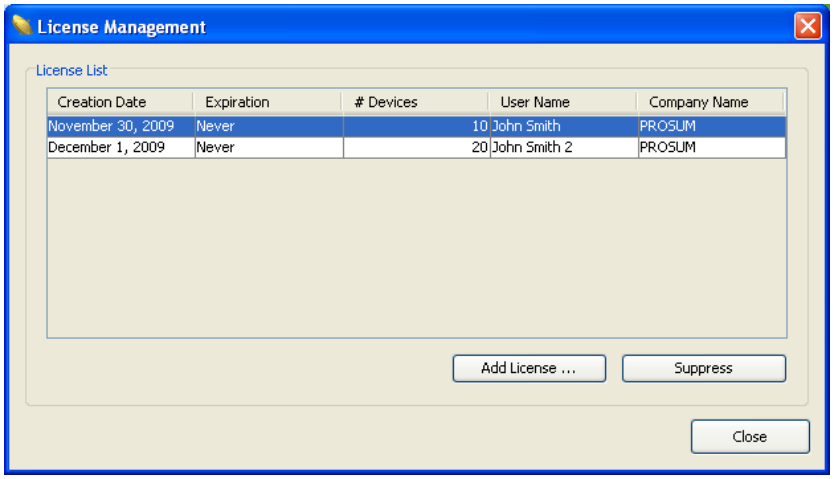

Figure 3: List of Licenses

Each license line displays the following information:

Creation Date	License creation date
Expiration	License expiration date. (It never expires unless it is a trial license)
# Devices	Number of devices provided by this user license
User Name	User name
Company Name	Company or organization name

To install a new license, click on the *Add License …* button. In the dialog box, fill in the complete license file path, and click *OK* to validate. Once the license file has been found and validated, the new license information should appear in the license list.

To delete a license from the license list, click *Suppress*. You must confirm the license suppression by providing the main password.

3.3 LICENSE APPLYING RULES

- If one or more purchased licenses are installed and the USB key is not detected, licenses become trial licenses expiring seven days after the INSTALLATION date.
- If trial and purchased licenses are installed simultaneously, only purchased licenses are taken into account. The trial licenses are ignored.
- When several licenses are installed, PRIMA Center can manage the sum of the devices allowed by each license.

4 MAIN PASSWORD

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

The default password is **superu**.

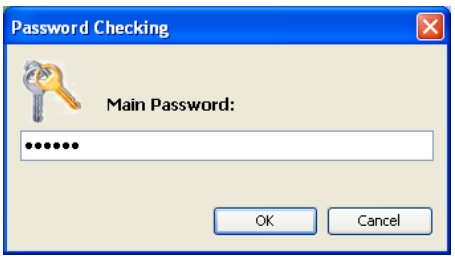

Figure 4 - Main Password Checking Dialog.

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.

5 DEVICE PANEL

5.1 DETECTING DEVICES

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

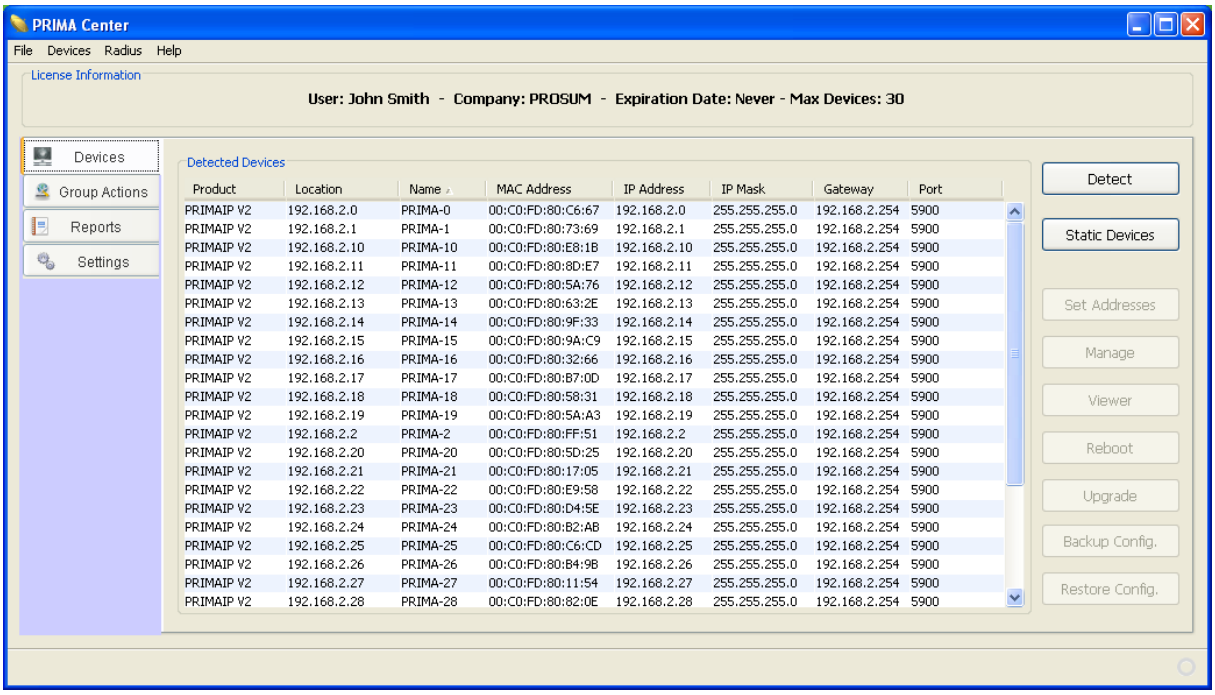

Figure 5 – Device Panel

PRIMA Center 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 PRIMA Center 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 PRIMA Center.

Note: To detect dynamic devices, PRIMA Center 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 PRIMA Center application.

Each line of the device list displays the following information:

Product	Identifies the product type
Location	IP address or host name as detected by PRIMA Center. This field may be different from the IP address of static devices
Name	Device name as configured in the device management
MAC Address	Unique Ethernet address reported by the device
IP Address IP Mask Gateway	IP settings of current device
Port	BASE of the range of TCP/IP ports used by the device for management and viewers

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

5.2 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.

5.2.1 DETECT

This button launches the device detection process. By this action, PRIMA Center 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

5.2.2 STATIC DEVICES

This button opens the Static Device Management box.

5.2.3 SET ADDRESSES

This button can be used to temporarily modify the device 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:

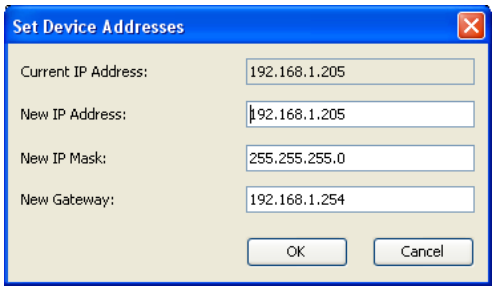

Figure 6 - Set Device Addresses Dialog

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: To modify these settings by using PRIMA Center, you must allow this action in the device management. You receive an error message if the device is not set up to allow PRIMA Center to perform this action. For further information, please refer to the device user's manual.

Note: All IP settings modified directly by PRIMA Center are only valid until the device reboot. You must run the device management for permanent settings. For further information, consult the device user's manual.

5.2.4 MANAGE

This buttons launches your current browser so that it automatically tries to access the HTTPS management server of the selected device. Note that this is only possible if the device is running an HTTP server. For example, the DSNet Broadcaster is supported by PRIMA Center but is not managed by HTTP. Click *Viewer* to open the DSNet Management.
Note that when accessing the device management by this way, you bypass the user/password authentication phase that is automatically implemented by PRIMA Center. For better security, we recommend you set up a global password for this action. See Security Settings.

5.2.5 VIEWER

This button launches the KVM switch viewer currently installed if the device is an IP KVM. This viewer may be a Windows application if PRIMA Center is running on a Windows system or a Java application if PRIMA Center is installed on Windows or another system. To select the Viewer application, go to *Device* Settings in the *Settings* panel.

5.2.6 REBOOT

This button permits to reboot the selected device. Following this action, the detection of the rebooted device can take a couple of minutes.

Note: You can configure a password to set this action in the security tab of the *Settings* panel.

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

5.2.7 UPGRADE

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

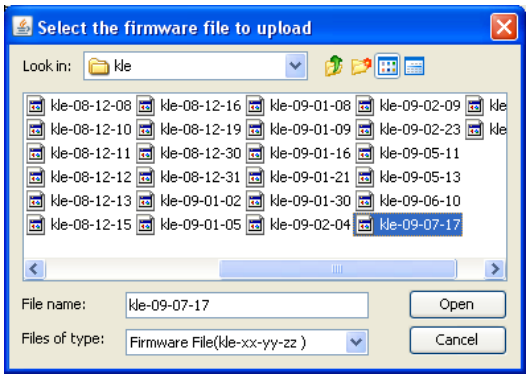

Figure 7 - Firmware File Selection Dialog

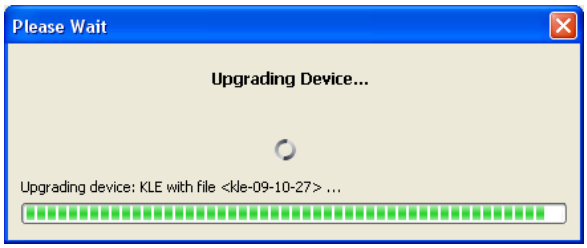

Figure 8: Upgrading Device

Note: You can set a password to protect this action in the *Security* tab of the *Settings* panel.

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

5.2.8 BACKUP CONFIG

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

Note: You can set a password to protect this action in the *Security* tab of the *Settings* panel.

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

5.2.9 RESTORE CONFIG

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

Note: You can set a password to protect this action in the *Security* tab of the *Settings* panel.

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

6 GROUP ACTION PANEL

This panel permits you to apply some actions to more than one device simultaneously. An action can be performed on all devices or on a subset of selected 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).

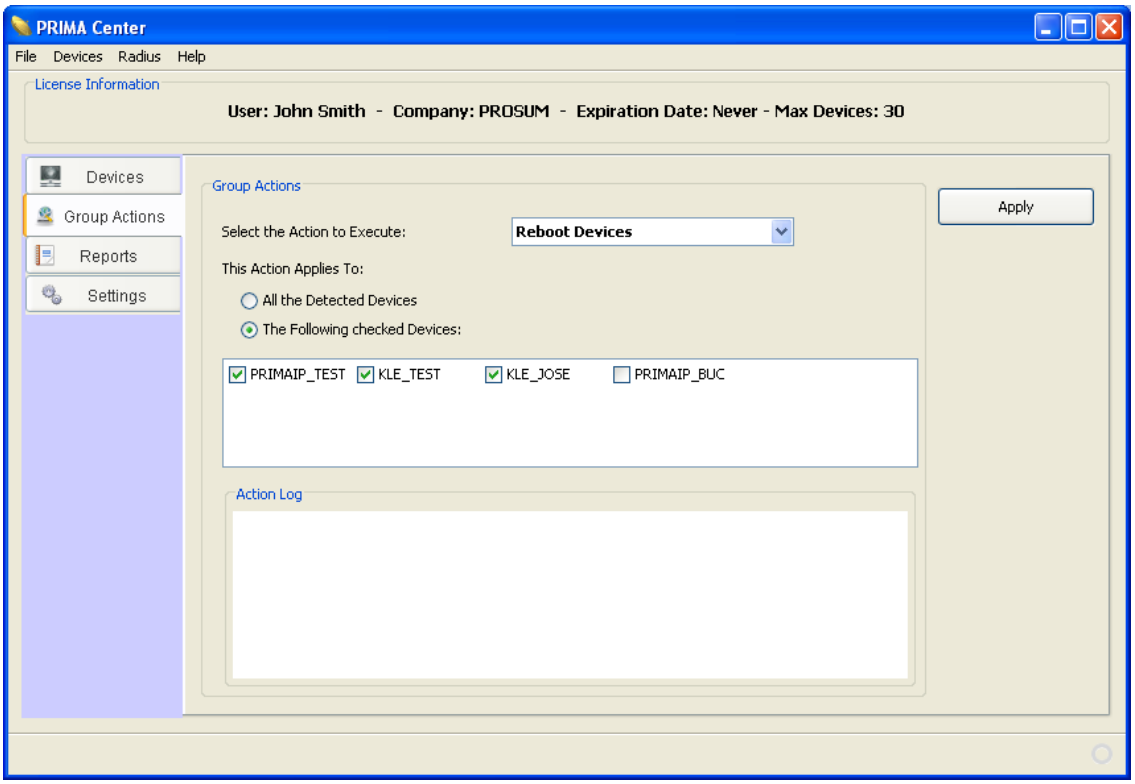

Figure 9 - Group Actions Panel

Select the type of action you wish to apply, select *All the Detected Devices* or select *The Following 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: You can set up a password to protect group actions by clicking the *Security* tab of the *Settings* panel.

7 REPORT PANEL

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

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

7.1 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 PRIMA Center applications that contact them. Log messages contain no security sensitive information.

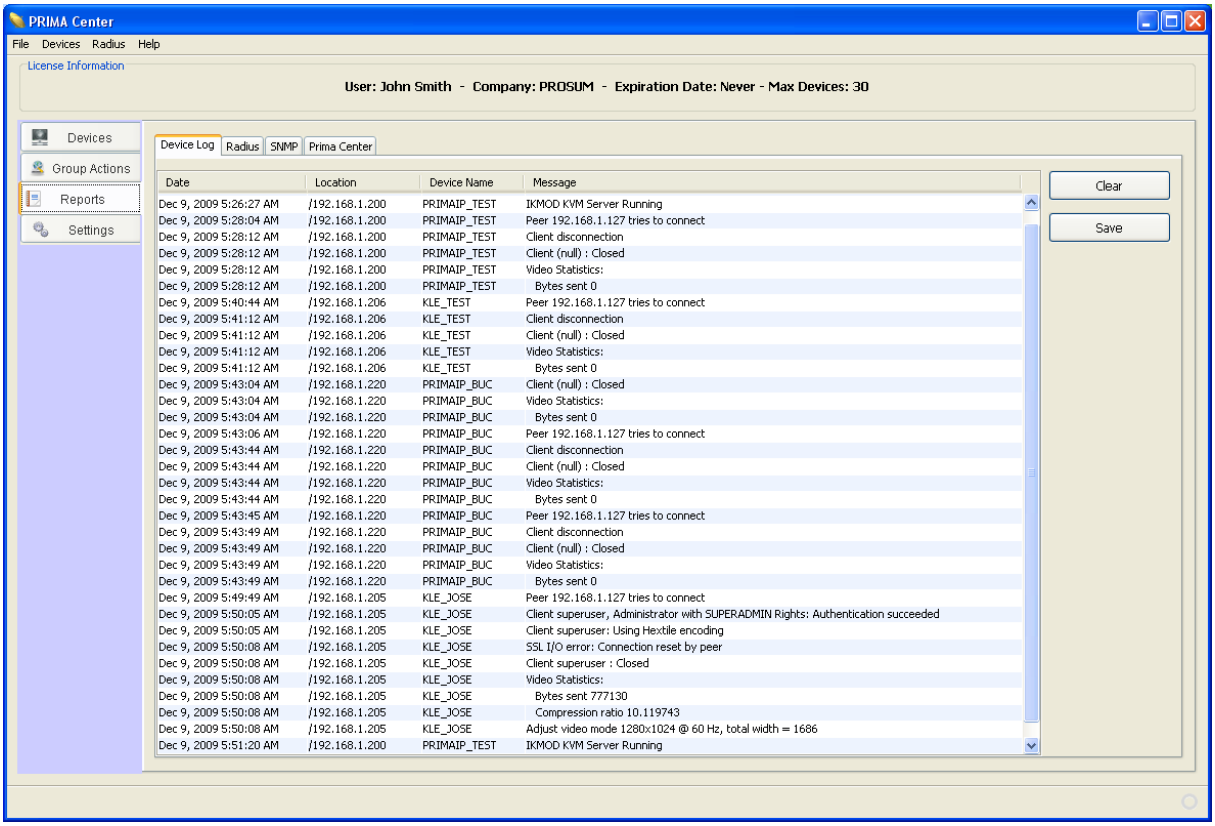

Figure 10 – *Device Log* Tab *of* Report Panel

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\.PRIMA Center\Reports\
  - USER_HOME stands for the user's home directory.

7.2 RADIUS ACCOUNTING LOG

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

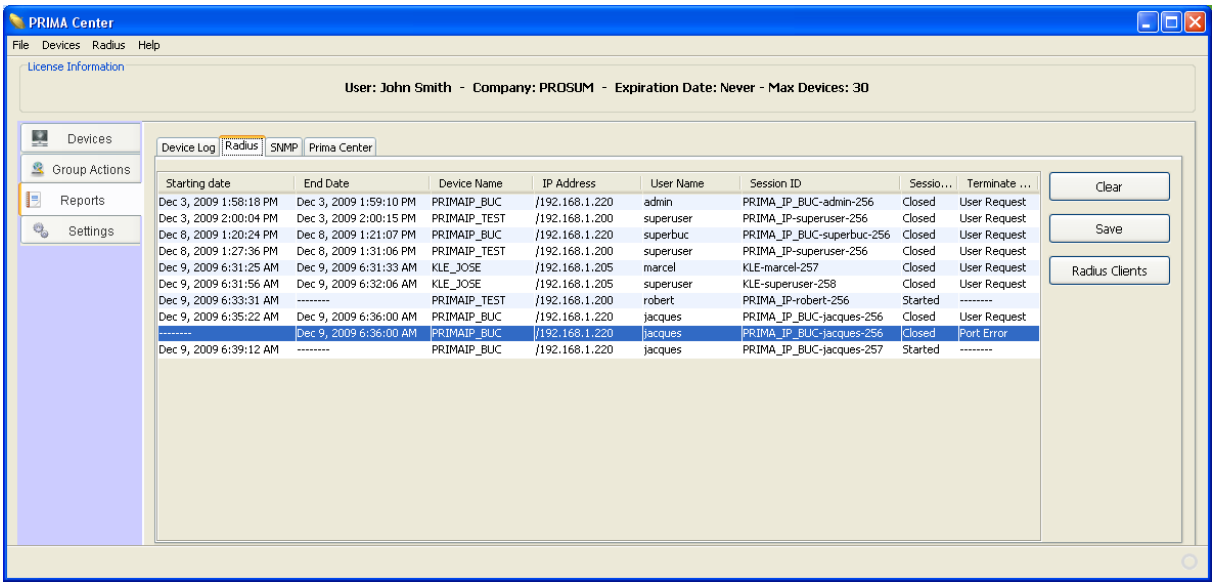

Figure 11 - Radius Accounting Log

PRIMA Center includes a Radius Accounting server able to receive the Radius Accounting messages sent by all devices. The devices must be set up to send their messages to the IP Address of the computer running PRIMA Center. You must also add all devices either to the *Static* Devices *List*, or to the *Radius Client List* of PRIMA Center. 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\.PRIMA Center\Reports\" folder - USER_HOME stands for the user's home directory.
- Radius Clients opens the radius client management box. See Radius Client Management.

7.3 SNMP LOG

PRIMA Center 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 PRIMA Center.

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

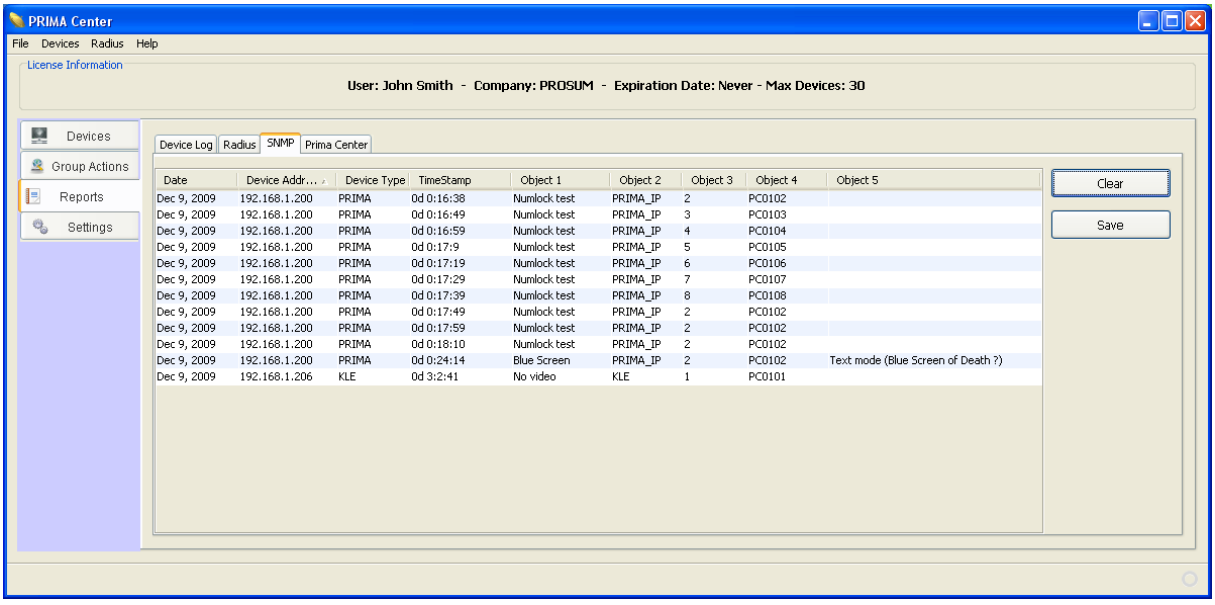

Figure 12 - SNMP Log Tab

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\.PRIMA Center\Reports\"* folder - *USER_HOME* stands for the user's home directory.

7.4 PRIMA CENTER LOG

You can see under this tab the messages of PRIMA Center itself.

8 SETTINGS PANEL

The *Settings* panel is the place where you can configure PRIMA Center 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.

8.1 DEVICE SETTINGS

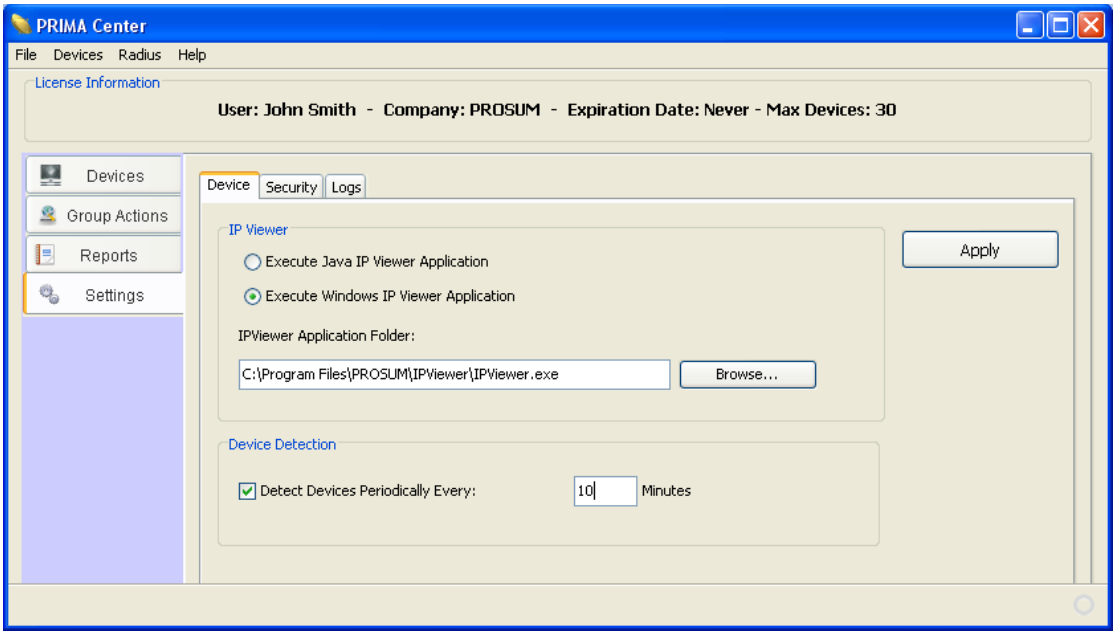

Figure 13 - Device Setting Panel

8.1.1 IP VIEWER

If PRIMA Center 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 PRIMA Center 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.

8.1.2 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.

8.2 SECURITY SETTINGS

The purpose of Security settings is to improve the device protection concerning some critical actions. You can ask PRIMA Center to add an authentication dialog before performing these individual or group actions.

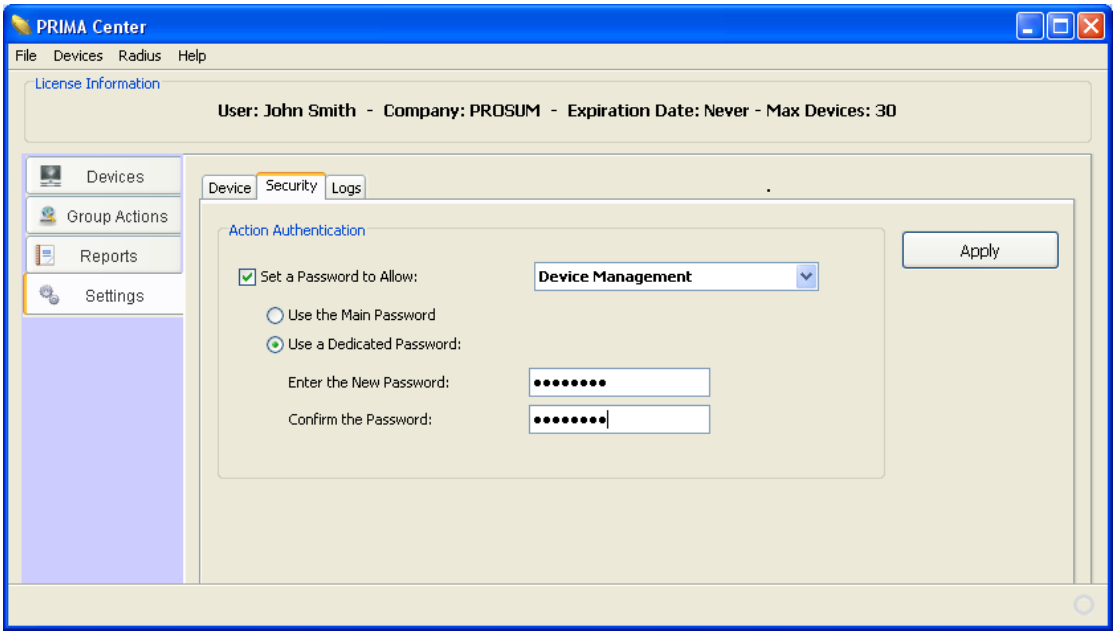

Figure 14 - Security Settings

The actions concerned by this protection are:

- Device management
- Device reboot
- Firmware upgrade
- Configuration backup and restore

First select the action to be setup in the list. Check *Set a Password to Allow* to force a password request for this action. It can be the main password or a different specific password for each action. Select *Use the Main Password* or *Use a Dedicated Password* according to your wish. In case of dedicated password, fill in *Enter the New Password* and *Confirm the Password*. Click *Apply* to validate your modifications for each selected action.

8.3 LOG SETTINGS

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

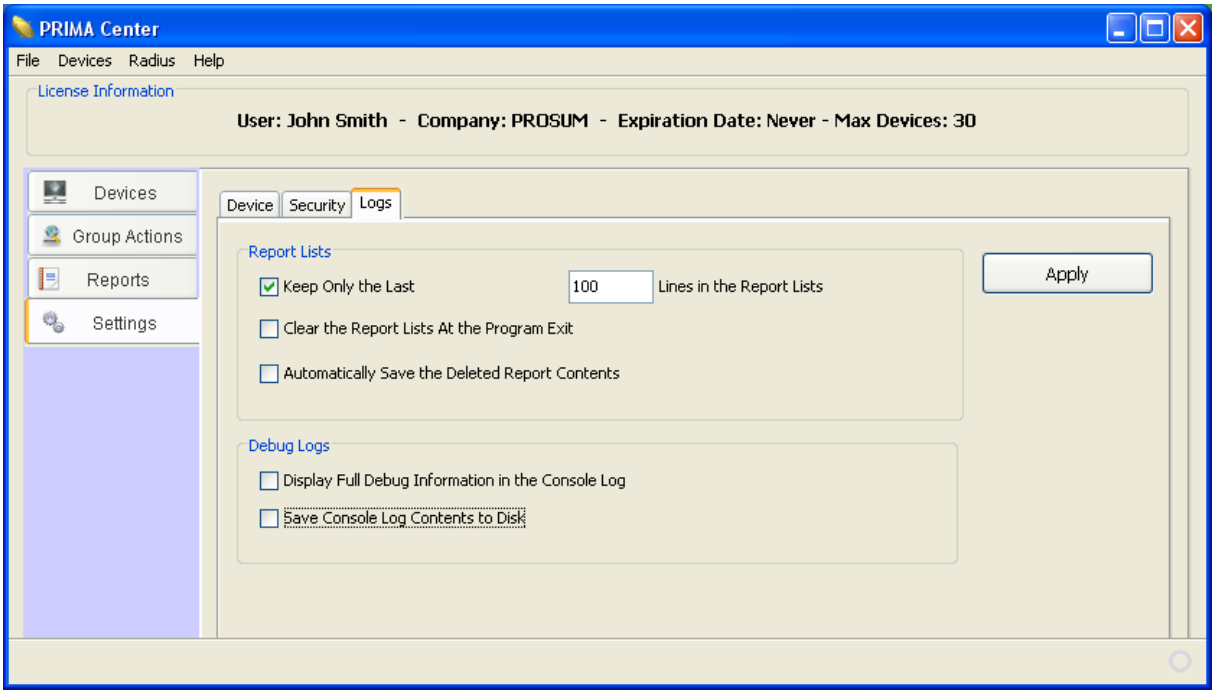

Figure 15: Log Settings

8.3.1 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

8.3.2 DEBUG LOGS

By default, PRIMA Center 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, PRIMA Center 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\.PRIMA Center \Debug" folder

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

9 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:

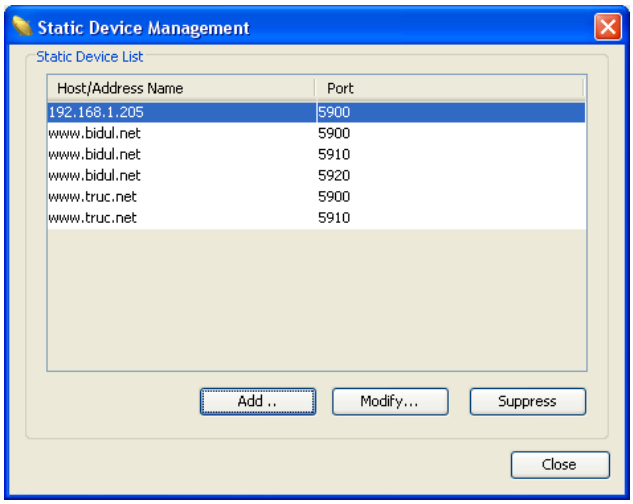

Figure 16 - Static Device Management

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:

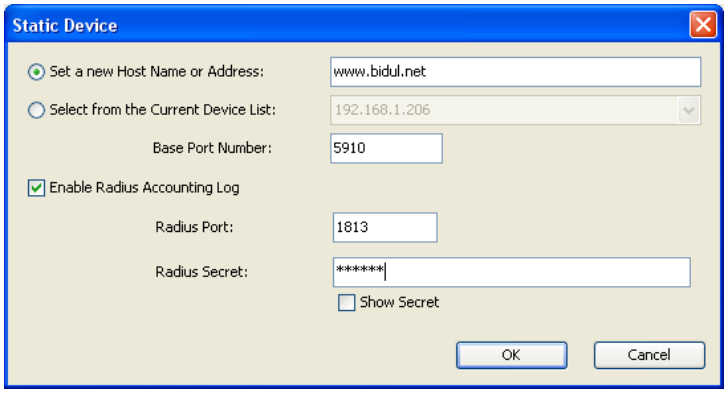

Figure 17 - Static Device Edit

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.

10 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.

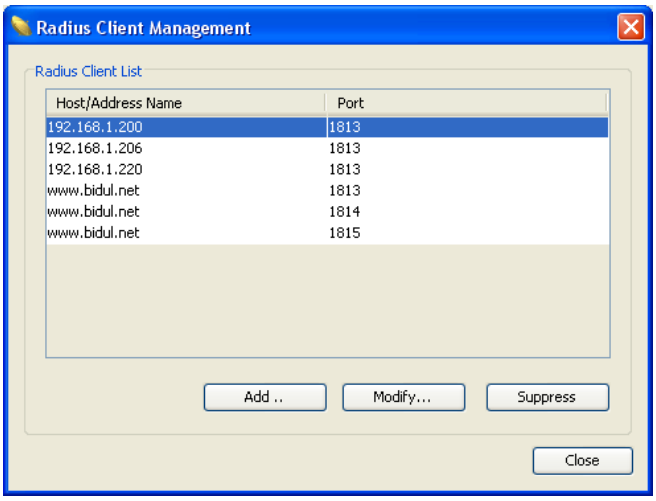

Figure 18: Management of Radius Client List

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

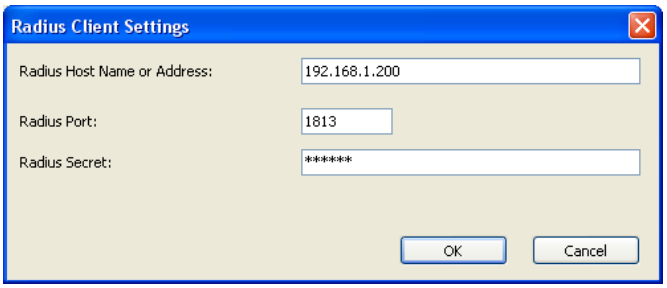

Figure 19: Radius Client Settings

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