



User Guide

SUSIAccess

Remote Device Management

Edition 2.0
May 10 2012

Part. No. **200EMBSA01**
Printed in Taiwan

Advantech SUSIAccess User Manual

ADVANTECH SUSIACCESS USER MANUAL	3
1. SOLUTION OVERVIEW	4
2. SOFTWARE STRUCTURE	6
3. INSTALLATION	7
1.1. SUSI ACCESS REQUIREMENTS	7
1.2. SUSIACCESS CONSOLE	8
1.3. SUSIACCESS CLIENT	10
4. USING SUSIACCESS.....	13
1.1. REMOTE MONITORING.....	18
1.2. REMOTE ON OFF	23
1.3. REMOTE KVM	28
1.4. SYSTEM RECOVERY	31
1.5. SYSTEM PROTECTION	35

Solution Overview

SUSIAccess®-Remote Device Management

Advantech has designed an industrial remote management program to provide our customers with remote device monitoring, desktop connection, system recovery and system protection features that will help customers to access multiple clients through a single console for remote device management. SUSIAccess will immediately recognize sudden equipment malfunctions and provide real-time equipment maintenance, as well as system security protection mechanisms that significantly improve maintenance efficiency. Plus, an active update feature will improve system stability and reliability.

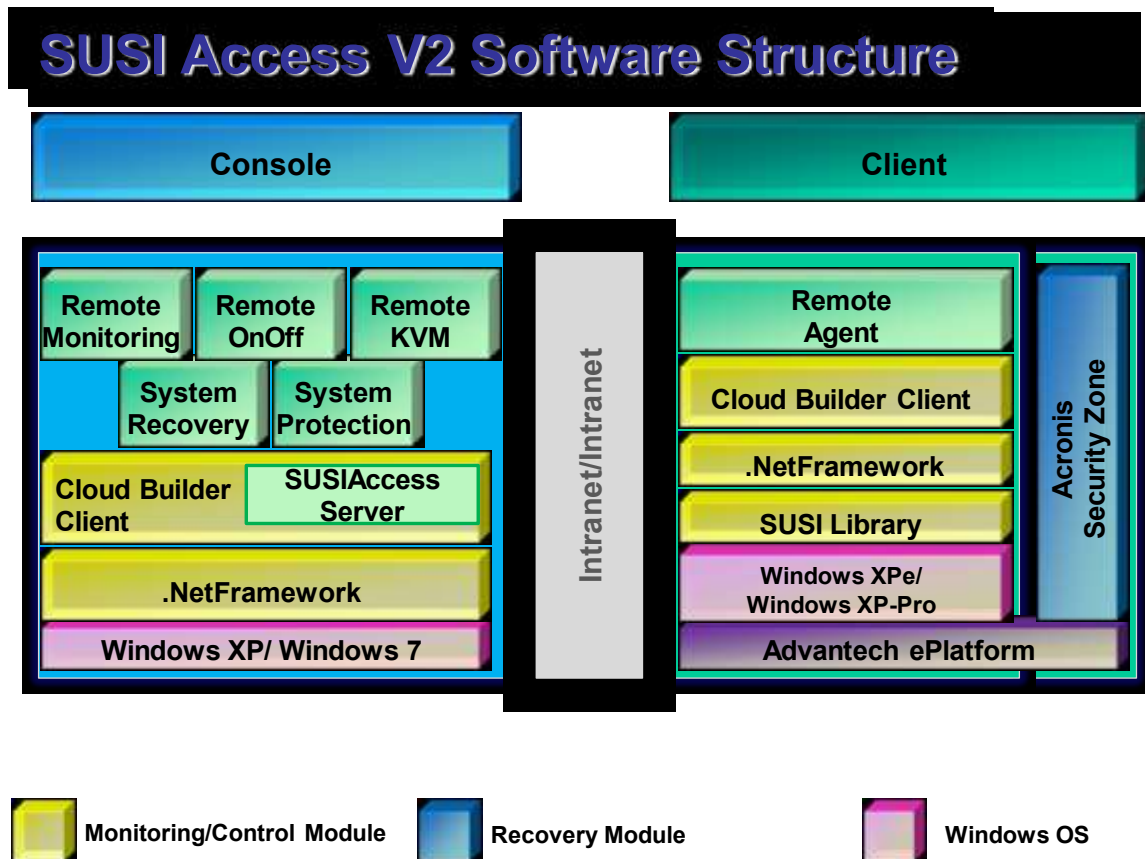


- ✓ **Remote Monitoring:** Monitors system status of remote devices, including hard disk temperature, hard drive health, network connection, system / CPU temperatures, system / CPU fan speeds and system voltages. Support for email alarms and function logs so that managers can regularly keep on top of their remote devices.
- ✓ **Remote On/Off:** Control on/off times according to each device, or pre-set time cycles to switch a device on/off. For example, a public service machine can be set for 6:00 am start and 23:00 pm shutdown. Ideal for night time and energy saving applications.

- ✓ **Remote KVM:** Controls the desktops of remote devices. IT technicians or maintenance engineers can manipulate a remote computer directly for maintenance and updates. Pre-configure settings without the need to enter individual IP, username and passwords—providing significant reduction in service times required.
- ✓ **System Recovery:** Controls system backup and restore of remote devices, or pre-set system backup types and restore times. For example, a bank ATM machine is set for system backup every Monday at 1:00 am. If a system crashes, you can immediately gain access via the remote console, and perform a system recovery so that the equipment maintains normal operation. (System recovery programs use Acronis True Image backup and restore technology which must be installed before use.)
- ✓ **System Protection:** Controls remote equipment, system protection and monitoring, and security. If a machine is threatened by a virus, the program will automatically detect and prevent intrusions.
*System Saver program integrates McAfee's Embedded Security System Protection program which must be installed before use.

1. Software Structure

SUSIAccess includes two parts: Console and Client. Below is the communication structure:



- **SUSIAccess Console:**

The main program to manage all connected clients—a service program that auto-runs after Windows boots up.

- **SUSIAccess Client:**

The client side program to sync data with the server. This is a service program that auto-runs after Windows boots up.

Note: If you enable System Recovery, it will create an Acronis Security Zone, which is used for Arconis' recovery mechanism. When a system crashes or fails, the backup image in Acronis Security Zone will be available to recover the system.

Installation

1.1. SUSI Access Requirements

SUSIAccess Console:

Operating System: Windows XP 32-bit, Windows 7 32-bit (Windows 7 64-bit by project)

Software: Microsoft .NET Framework 2.0 or higher

SUSIAccess Client:

Operating System: Windows XP 32-bit, Windows 7 32-bit (Windows 7 64-bit by project)

Software: Microsoft .NET Framework 2.0 or higher

Driver: Advantech SUSI Software API or iManager2.0 API *

3rd party application: Acronis TrueImage 11, & McAfee Embedded Security, Solidifier V6.0

Note: For remote monitoring will need to install the latest version of SUSI software API or iManager on your client side to get the system/CPU temperature, fan speed and voltages, please go to Advantech Industrial Cloud Center (Click on the upper right of SUSIAccess) to download SUSI/iManager manually. Or go to Advantech support website, and use the platform name to download it.

1.2. SUSIAccess Console

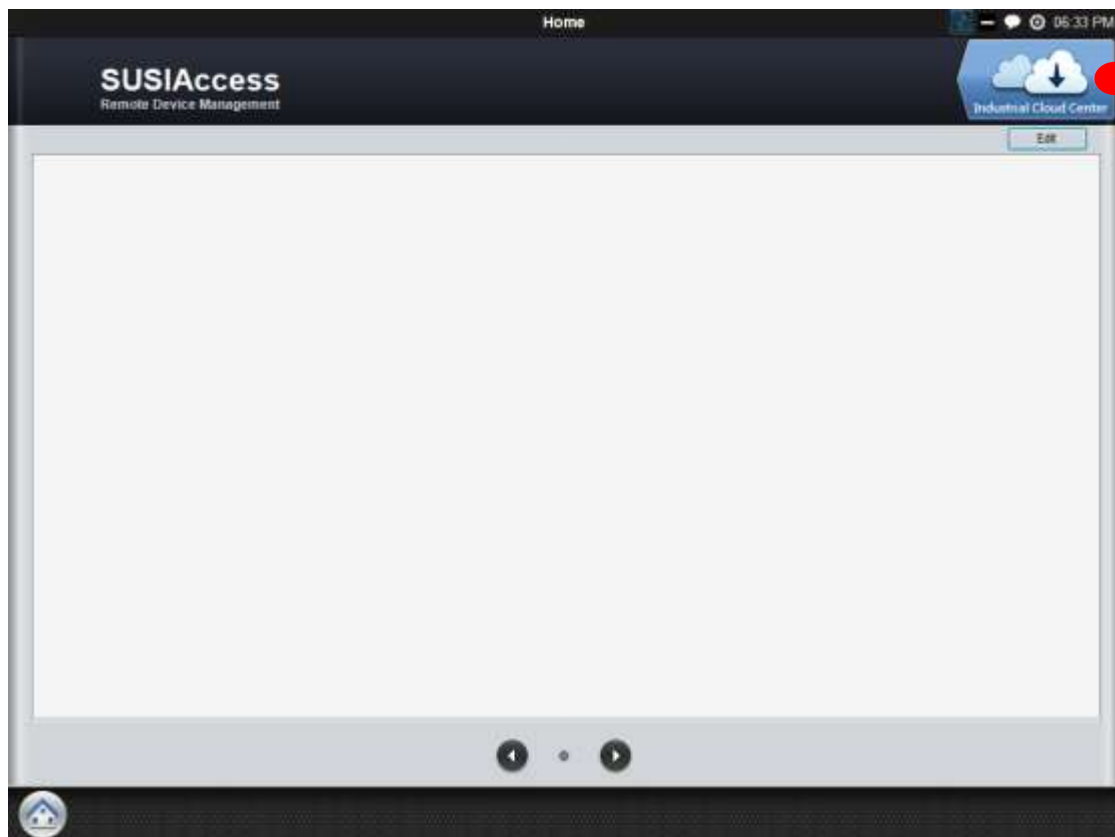
SUSI Access Console acts as a server for the clients. That means the device running SUSIAccess console will get all the health and status information from the SUSIAccess clients. The Console needs to be available by clients over a network.

To launch the SUSIAccess Console,

Click Windows Start Menu → All Programs → SUSIAccess.

SUSIAccess GUI is shown below.

Click on Industrial Cloud Center at the upper right corner:



● Advantech **Industrial Cloud Center**

Advantech **Industrial Cloud Center** now has 3 categories: Platform Utilities, iManager, SUSIAccess,

Click the Advantech **Industrial Cloud Center** button to download the SUSIAccess APPs.



Click Install to download and install the SUSIAccess APPs.



1.3. SUSIAccess Client

To launch the SUSIAccess client, click on the **Agent** App.

The Agent APP is also available from the Advantech Industrial Cloud.

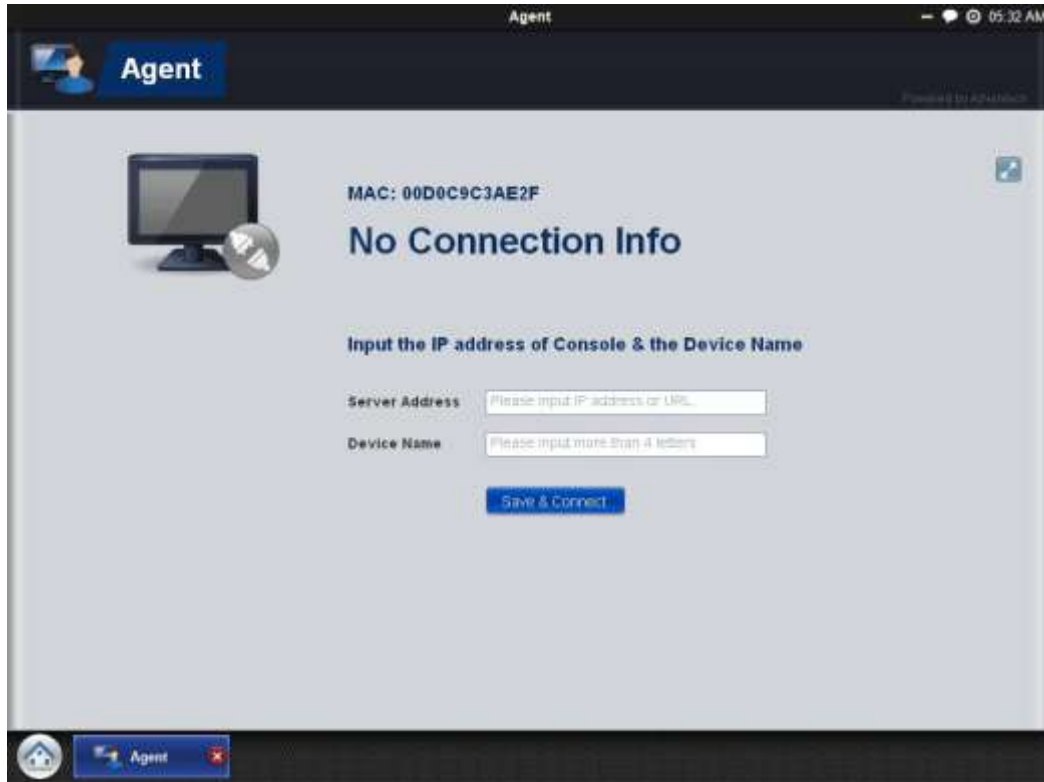


Agent (Client Side)

When starting Agent APP, it will ask for your server IP address. Your Server is the device which has the SUSIAccess Console Running. The Device name should be meaningful enough so you know exactly which Machine you are connecting if you have several clients

Server Address: Set IP Address, eg: 192.168.0.7

Device Name: Set Device Name, eg: Advantech Factory SMT Machine 1



Check the "Save & Connect", the agent will connect to the SUSIAccess Console server.

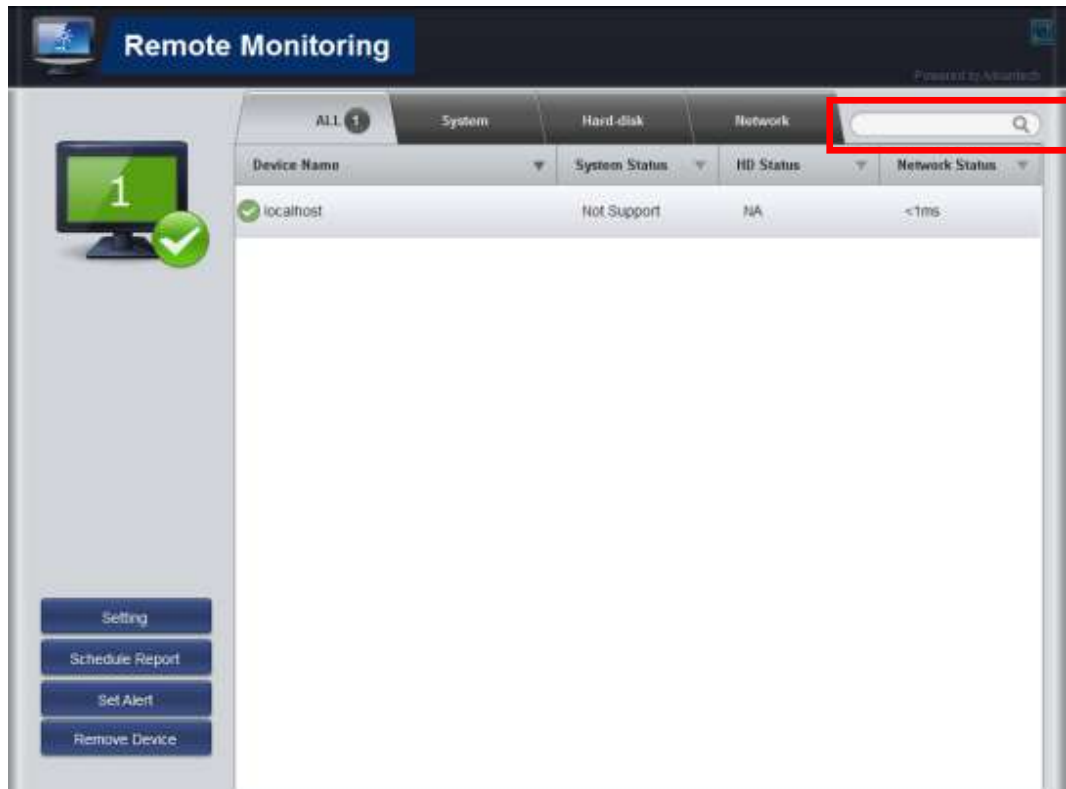


Using SUSIAccess

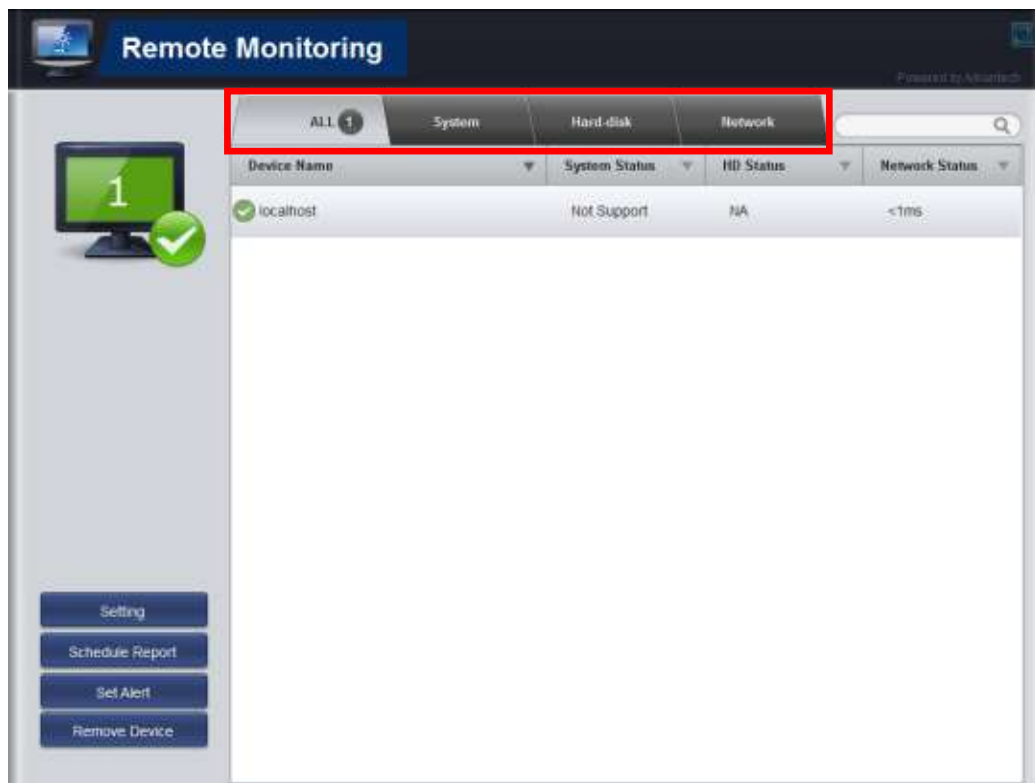
SUSIAccess is for remote device management. Right now, we have 5 Remote Apps and will have more in the future. We've designed them in same style for easy use. Let's have a look.

General User Interface

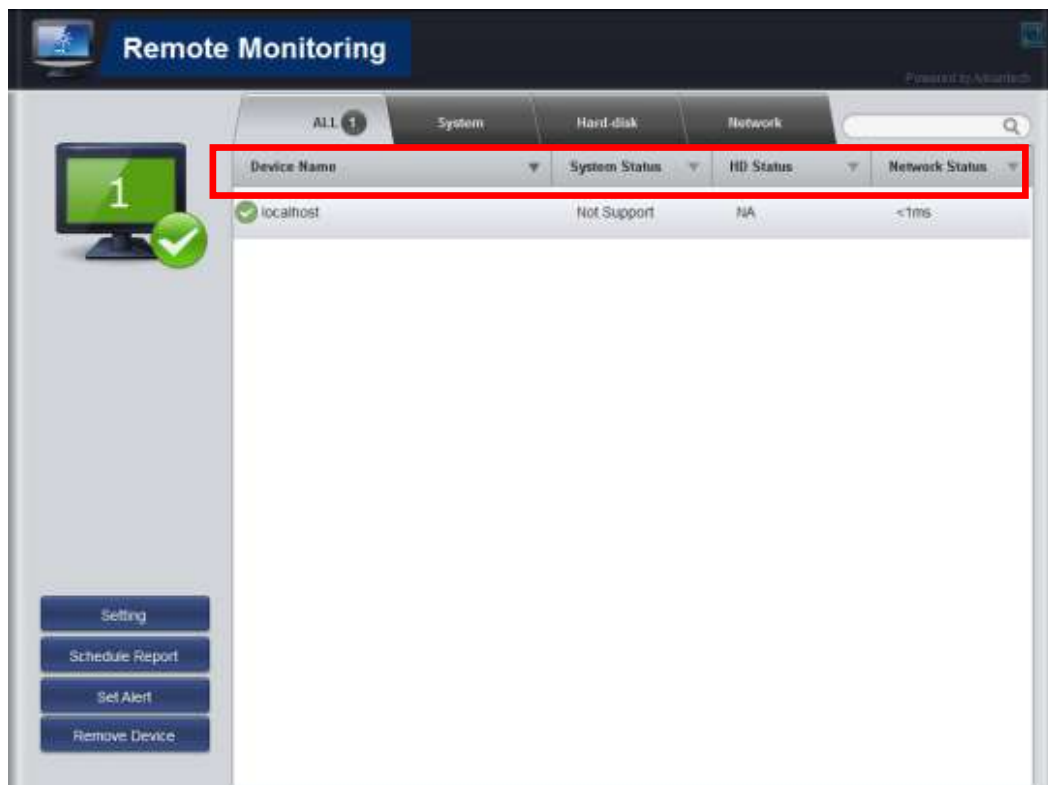
1. Search bar: Use it to easily search the device by Device Name. The list view will show the result instantly after you type each letter.



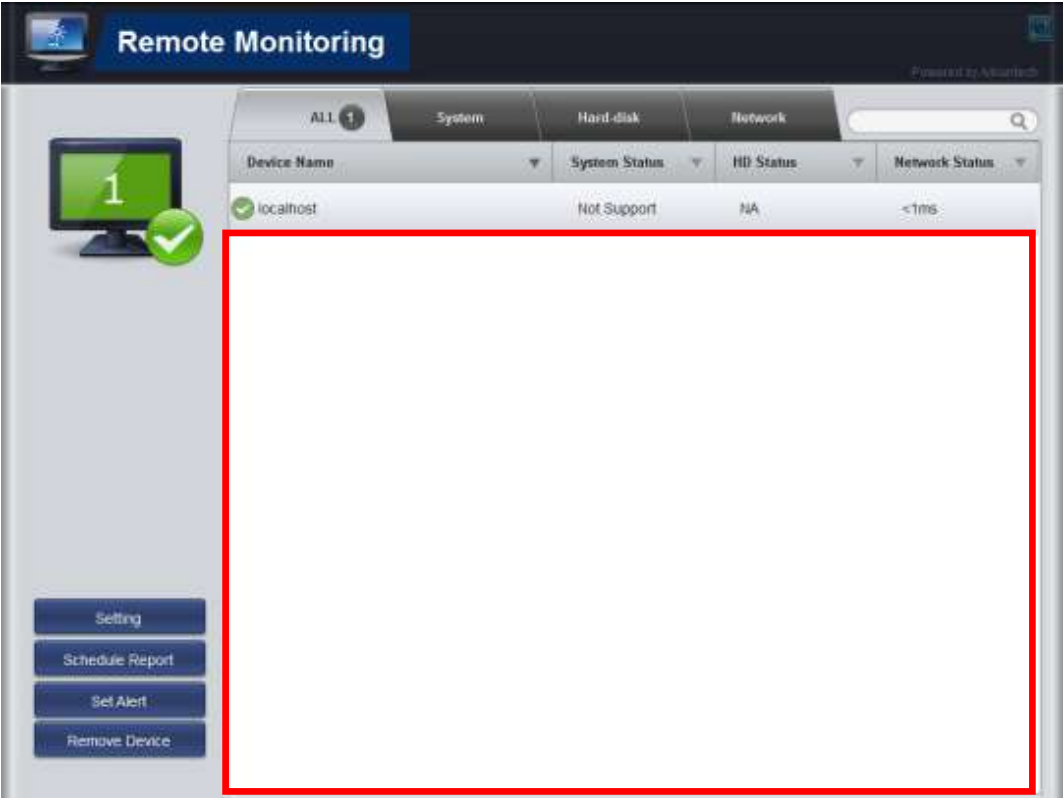
2. Group Tab: According to the information or functionality it can be divided into several tabs. The right of each tab will show the number of current devices.



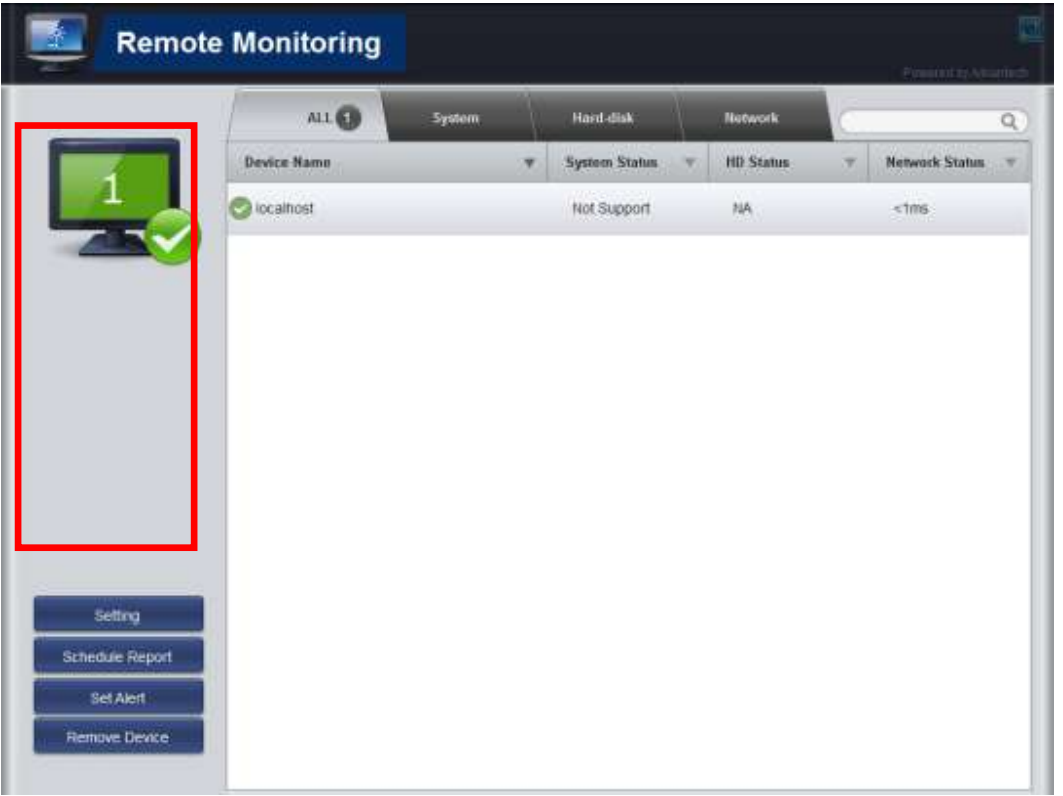
3. Sorting: Click on the column header to sort all the important information. The default is to sort by device name.



4. Device Item: Show all device items.



5. Status count : In addition to the number of devices that the tab shows, it shows the values that users most care about.

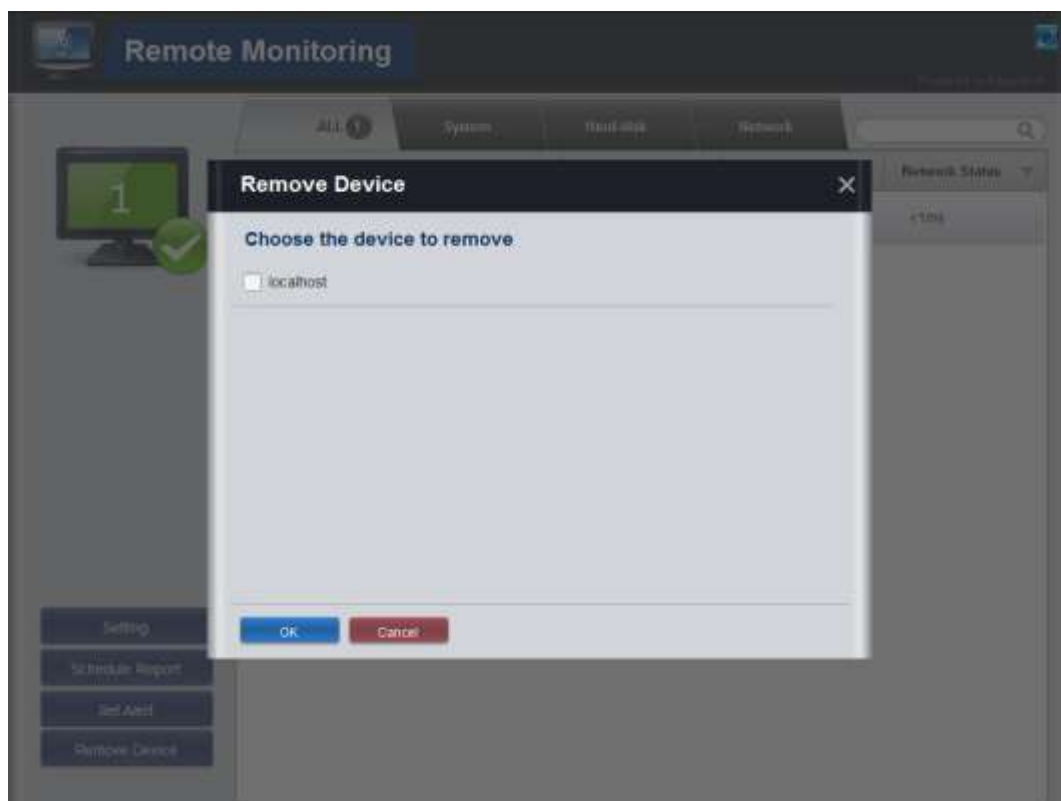


6. Extended function : Every Remote App has its own customized functions.



7. Remove devices.

If a device will be offline for some time and you don't want it show up, you can click on the **Remove Device** button to remove it. But if the device becomes active online again, it will show up again.



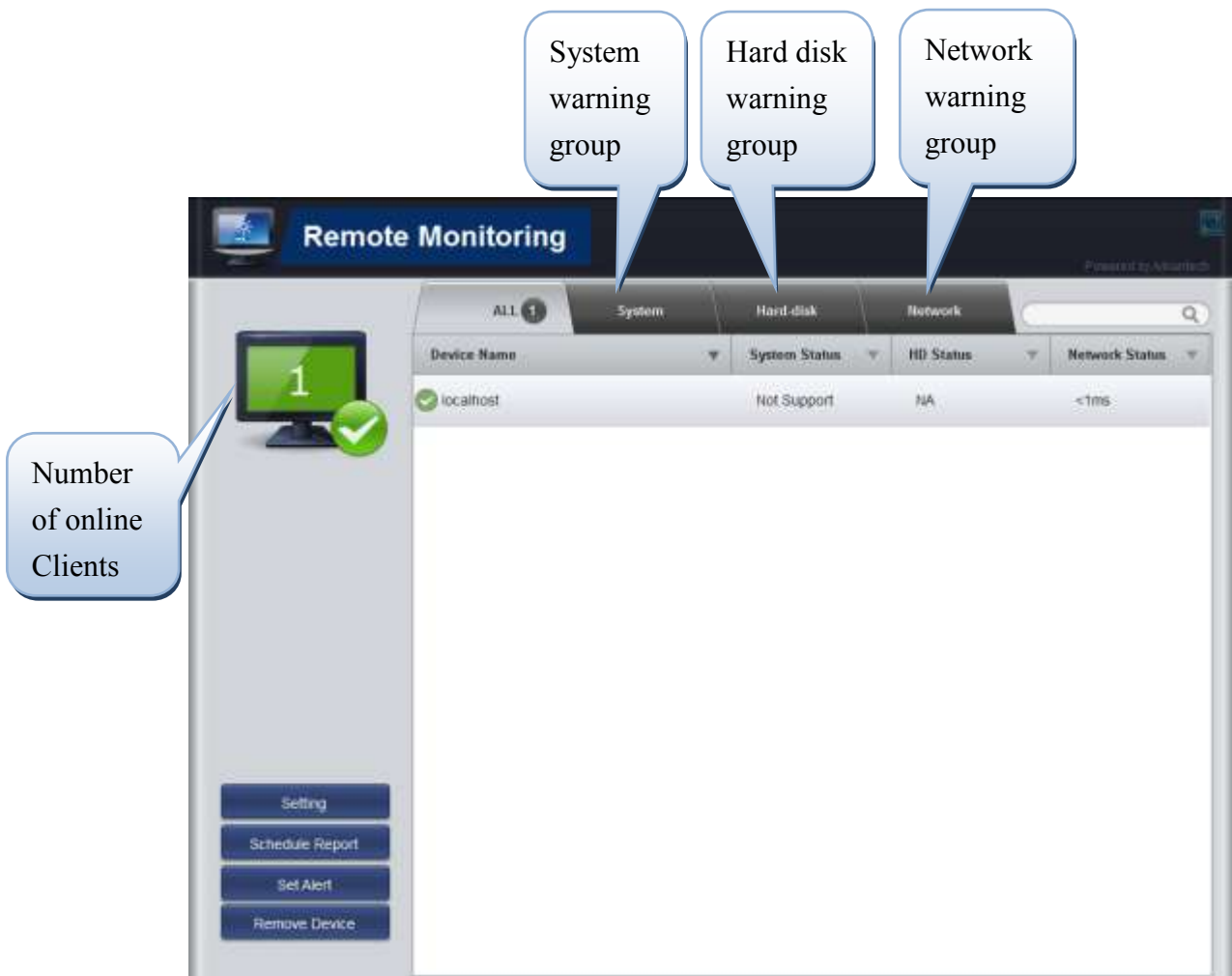
1.1.Remote Monitoring

Monitors the system status of remote devices, including hard disk temperatures, hard drive health, network connection, system / CPU temperatures, system / CPU fan speeds and system voltages. Email alarms and function logs are generated so that managers can regularly keep track of their remote devices.

Click **Remote Monitoring** icon to run the APP.



The main user interface.

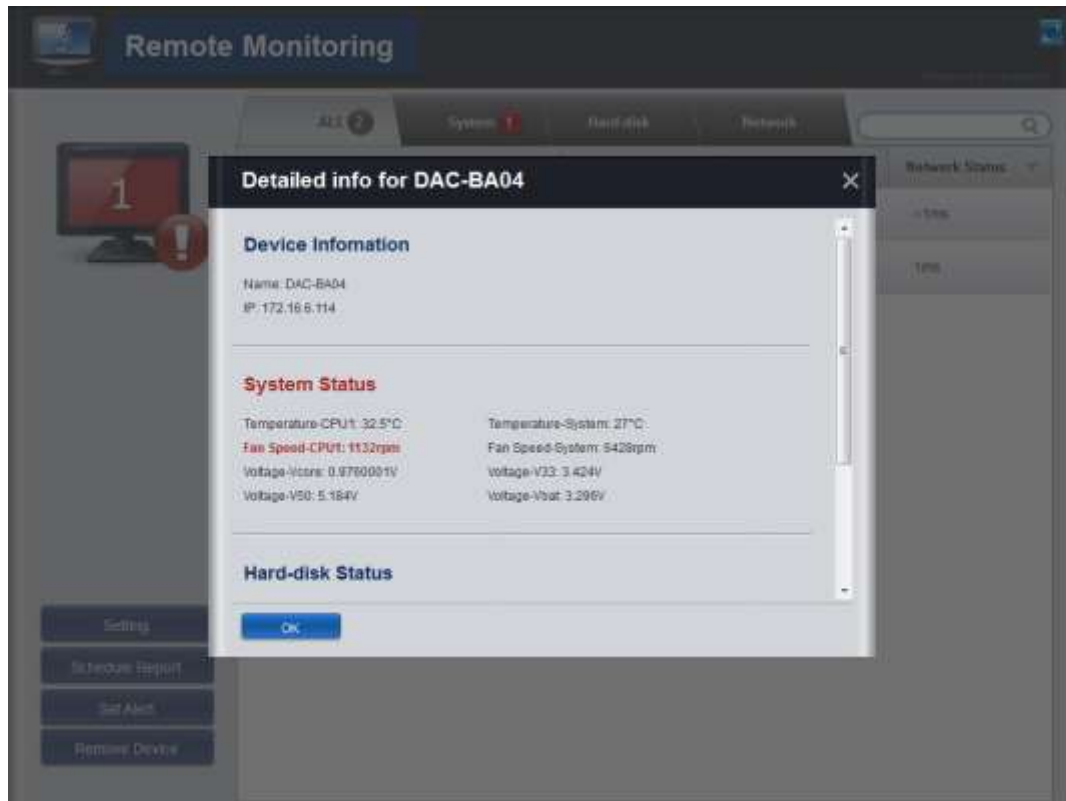


Setting: Sets the threshold of hardware monitoring

Schedule Report: Sets the report schedule, ex, daily, weekly or monthly

Set Alert: Sets the critical values for hardware monitoring

Double Click on the “device name”, ex: DAC-BA04 can show the detailed *Device Information* status:



Monitoring Threshold Settings

The **Setting** window for *Monitoring Threshold setting*, it contains four items: *Temperature*, *Fan Speed*, *Voltage*, and *Hard Disk*. In addition to the defaults, managers can increase or decrease items from this page.

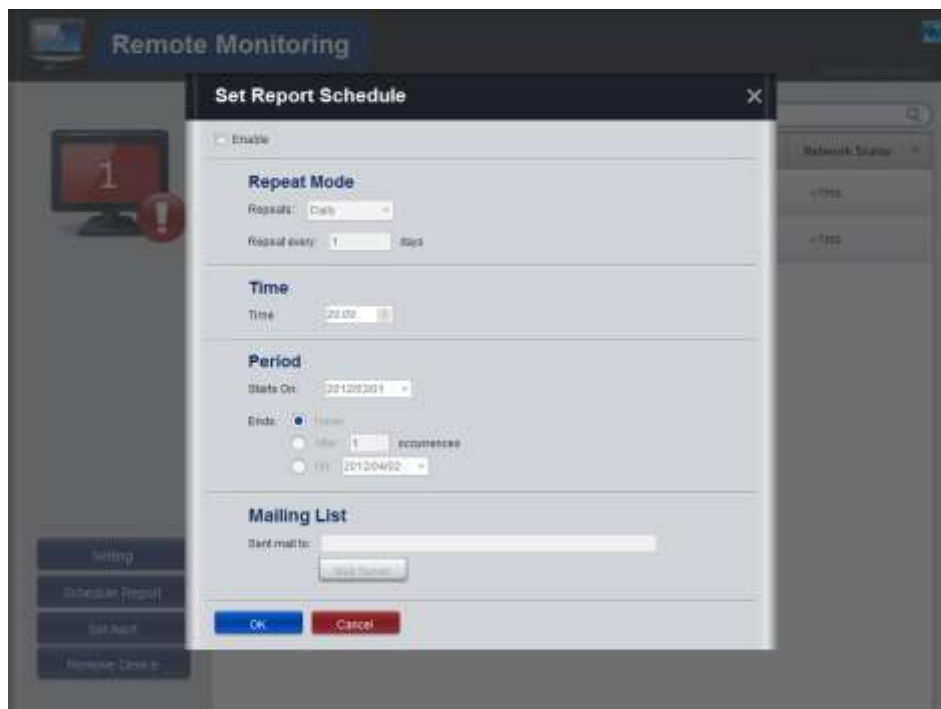


Set Report Schedule

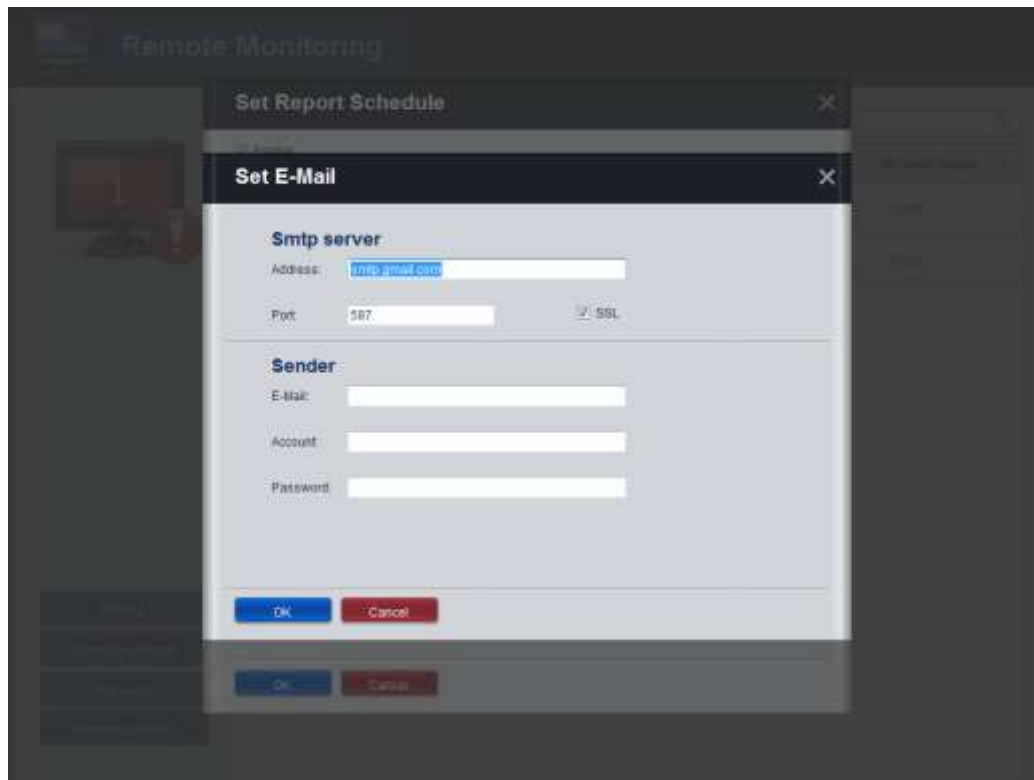
•This program's main function is for timings and runtime report status. The function is based on the information that you set in the **Set Report Schedule** window.

If you want to use timings for repeat functions, please follow the step-by-step instructions:

Click on the **Schedule Report** button to start, and set the *Repeat Mode*, *Time* and *Mailing List* recipient then press the **OK** button.

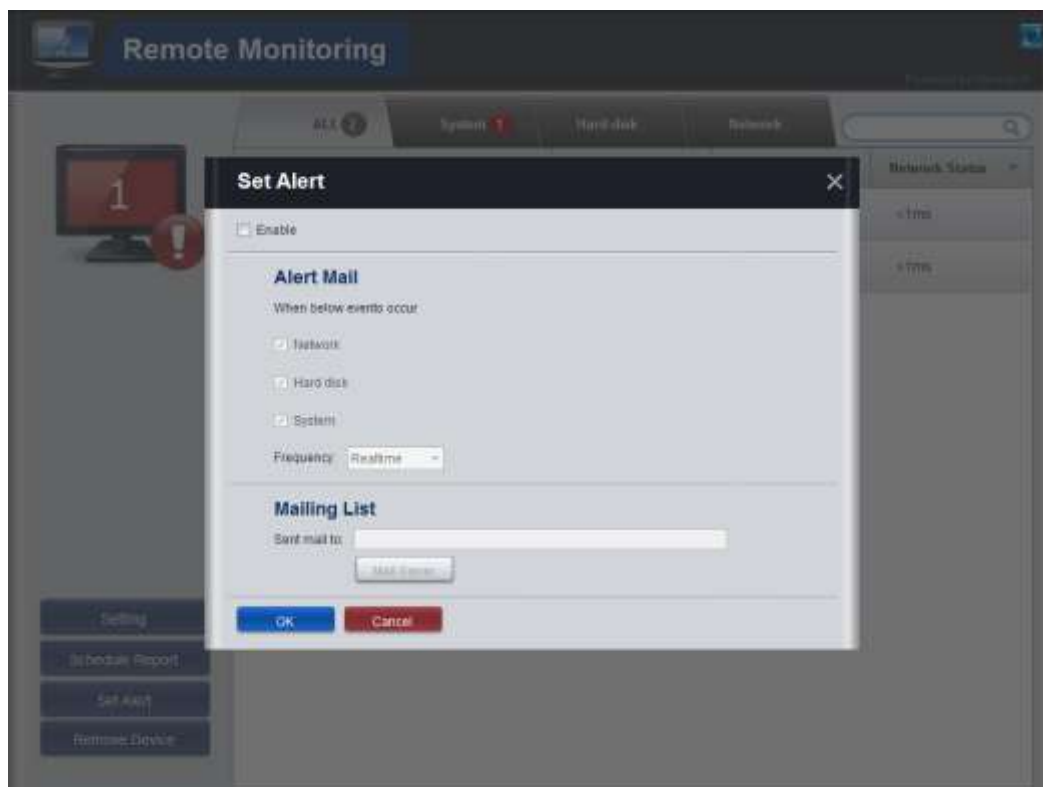


•Click in the **SMTP server** text-field, enter an address. If you use SSL (only provide SMTP mail setting currently), then set the sender's mail address, account and password. Finally, click on the **OK** button to finish your setup.



If you want to use the runtime alert function, please follow the step-by-step instructions:

Click on the **Set Alert** button and check the **Alert Mail** boxes, alert **Frequency** and recipient **Mailing List**.



- Click on **Mail Server** button under **Mailing List** to set it and then click OK.

1.2. Remote On/Off

Control on/off times according to each device, or pre-set time cycles to switch a device on/off. For example, a public service machine can be set for 6:00 am start and 23:00 pm shutdown, ideal for night time and energy saving applications.

Click the **Remote On/Off** icon to run the APP.



Below is the main screen for **Remote On/Off App**:



Power-On All: Power on all devices

Power-Off All: Power off all devices

Set Schedule: Pre-set schedule for all power on and power off

Remote ON/OFF function

Through the ON/OFF switch, you can control the power on/off status for the devices listed.


**Remote On/Off**

Powered by Advanced

2



0



Power-On All

Power-Off All

Set Schedule

Remove Device

ALL 2

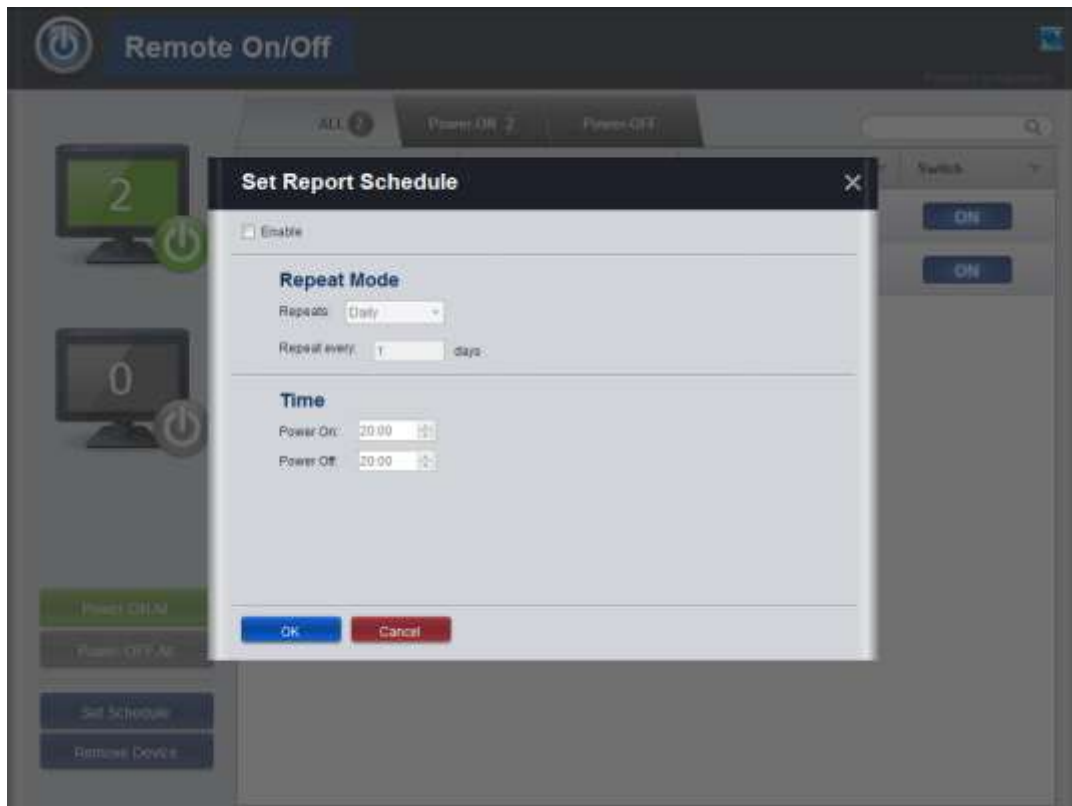
Power-ON 2

Power-OFF

Device Name	Working Period	Last Boot-up Time	Switch
localhost	9 hours	2012/04/02 09:10	ON
DAC-BA04	6 hours	2012/04/02 17:26	ON

Scheduling the Power On/Off Function

The program's main function is setting the timings for power on/power off. The function is based on the information that you set in **Set Report Schedule** in the Remote On/Off section. Users must enable the scheduled function and set the mode for **Power On/Power Off** that they want.



Wake On LAN

Wake-on-LAN (WOL) is an Ethernet computer networking standard that allows a computer to be turned on or woken up by a network message. The message is usually sent by a program executed on another computer on the same local area network. It is also possible to initiate the message from another network by using Subnet directed broadcasts or a WOL gateway service.

Requirements

A principal limitation of standard broadcast Wake-On-LAN is that broadcast packets are generally not routed. This prevents the technique being used in larger networks or over the internet. So WoL only work on the local network.

Wake-on-LAN support is implemented on the motherboard (BIOS) of a computer and the network interface (firmware), and is consequently not dependent on the operating system (and NIC drivers) running on the hardware.

The power supply must meet ATX 2.01 specifications.

In addition, in order to get Wake-on-LAN to work it is sometimes required to enable this feature on the network interface card or on-board silicon. Details of how to do this depend upon the operating system and the device driver.

Internet WoL solution

Subnet Directed Broadcasts (SDB) may be used to overcome WoL only for local network limitation.

SDB may require changes to intermediate router configuration. It is treated as normal network packets until processed by the final (local) router. This router converts the packet into a true broadcast packet. This technique allows a broadcast to be initiated on a remote network but requires all intervening routers to forward the SDB.

When preparing a network to forward SDB packets, care must be taken to filter such that only desired (e.g. WoL) SDB packets are permitted—otherwise the network becomes a participant in DDoS attacks such as the Smurf Attack.

Troubleshooting magic packets

Wake-on-LAN can be a frustrating technology to implement. This is because it requires appropriate BIOS, network card and, sometimes, operating system and router support to function reliably. In some cases, hardware may wake from one low power state but not from others. This means that due to hardware issues the computer may be waking up from the "fully off state" (S5) but doesn't wake from sleep or hibernation or vice-versa. Also, it is not always clear what kind of magic packet a NIC expects to see.

In that case, software tools like a packet analyzer can help with Wake-on-LAN troubleshooting as they allow to confirm (while the PC is still on) that the magic packet is indeed seen by a particular computer's NIC. The same magic packet can then be used to find out if the computer powers up from an offline state. This allows networking issues to be isolated from other hardware issues. In some cases they also confirm that the packet

was destined for a specific PC or sent to a broadcast address and they can additionally show the packet's internals.

In Windows Vista and higher, one can also determine how the OS was powered up. Running the `powercfg /lastwake` command in a CMD prompt will list the "Wake Source". The Wake-on-LAN event should also be logged in the System event log

1.3. Remote KVM

Controls the desktops of remote devices. IT technicians or maintenance engineers can manipulate a remote computer directly for maintenance and updates. Pre-configure settings without the need to enter individual IP, username and passwords—providing significant reduction in service times required.

Click the icon of Remote KVM to run the APP

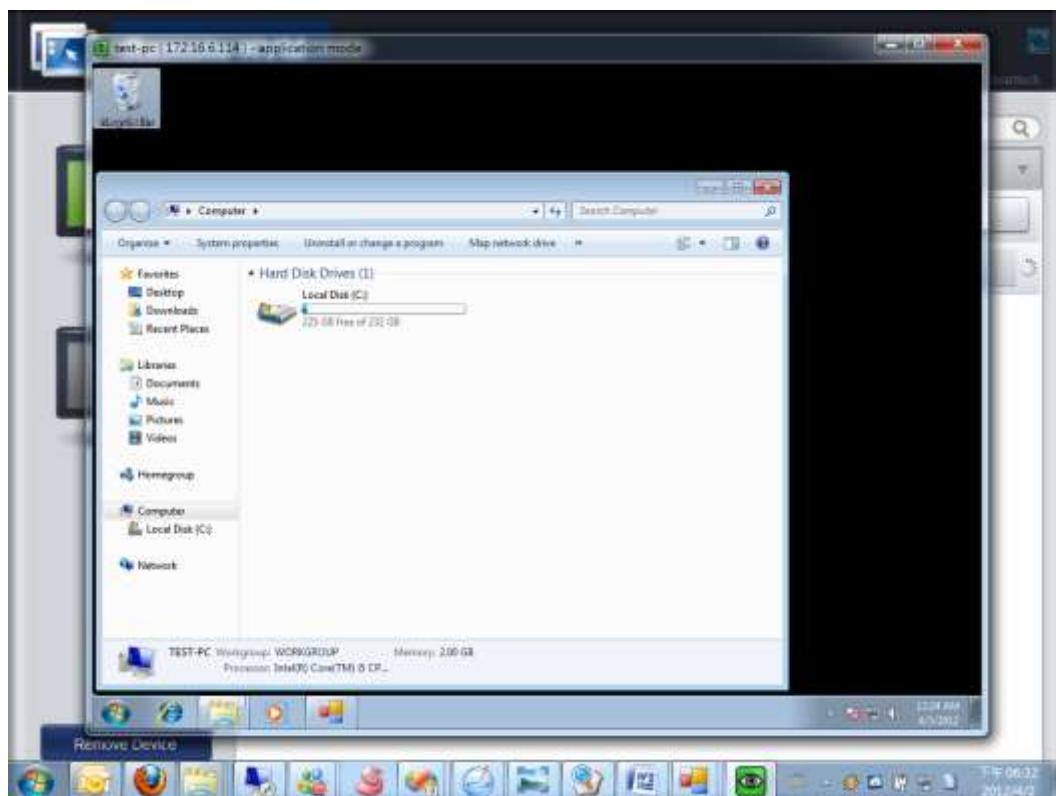
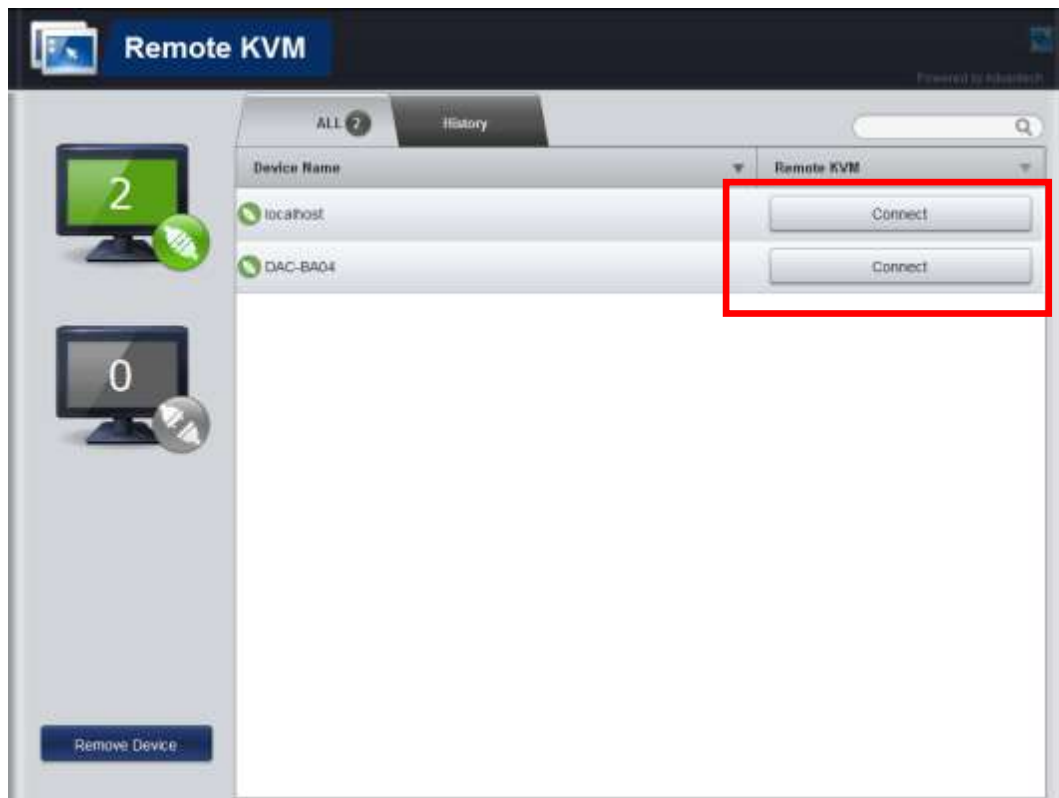


This is the main screen of the App.



Remote Desktop Control

Via the **Connect** button, you can run a remote desktop for the devices listed.



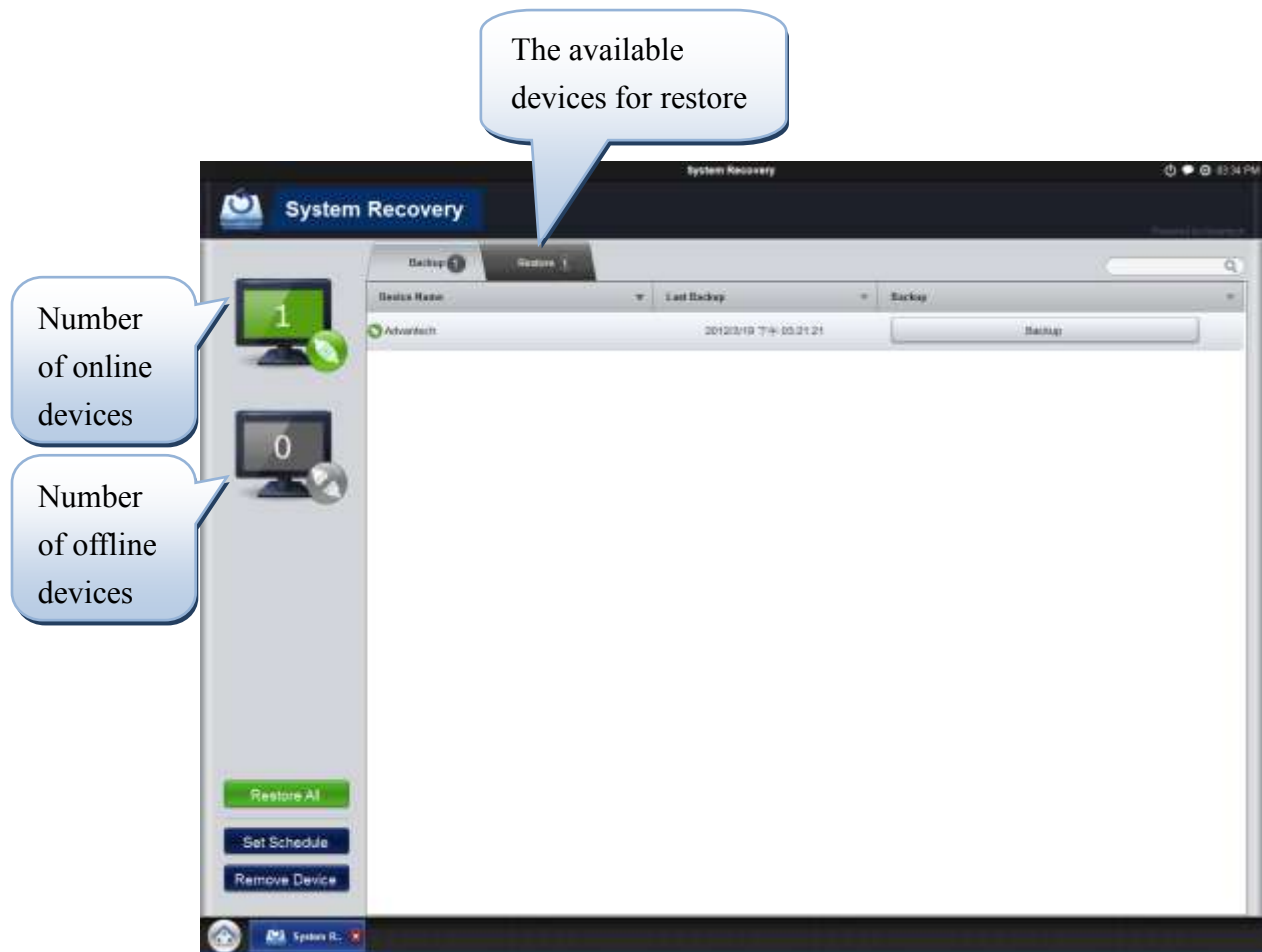
1.4. System Recovery

Controls system backup and restore of remote devices, or pre-set system backup types and restore times. For example, a bank ATM machine is set for system backup every Monday at 1:00 am. If a system crashes, you can immediately gain access via the remote console, and perform a system restore so that the equipment maintains normal operation. (System recovery programs uses Acronis True Image backup and restore technology which must be installed before use.)

Click the **System Recovery** icon to run the APP.



This is the default System Recovery screen, without any Clients connected.



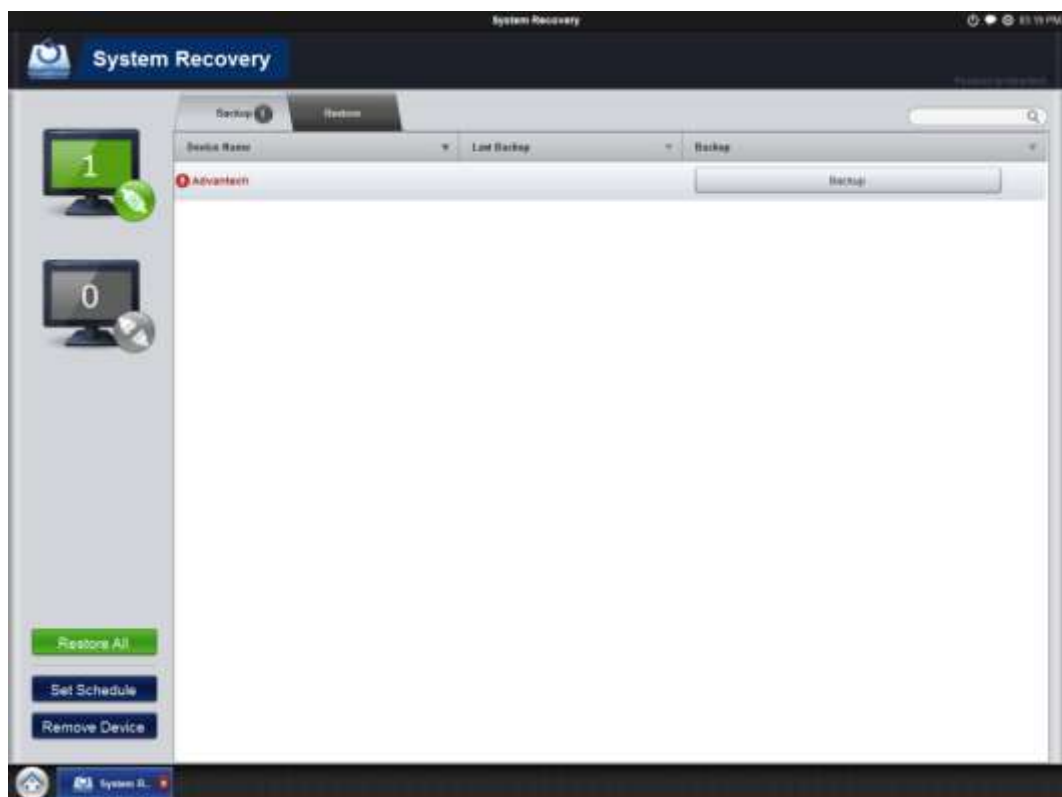
Restore All: Restore the OS for all connected devices

Set Schedule: Pre-set the backup schedule

If the client connects to the server, it will show the following screen, and point out the status of the Client. For example, this screen shows the Client name is “Advantech”, it is protected, and has no warnings.

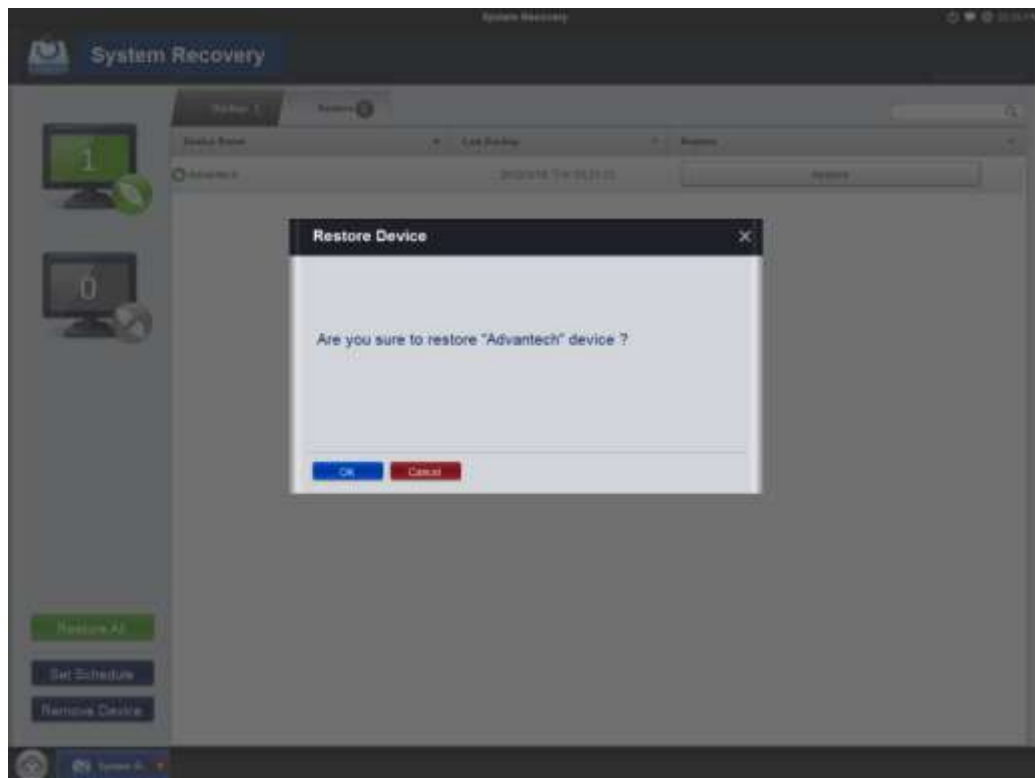


If the **Backup** button is clicked, the client will send the results of the backup to the console. If backup fails, you will get a red message; otherwise, you will get the last backup date





If you want to restore the last backup, please click the Restore Tab, and then click the **Restore All** button and then click **OK** to complete.



1.5. System Protection

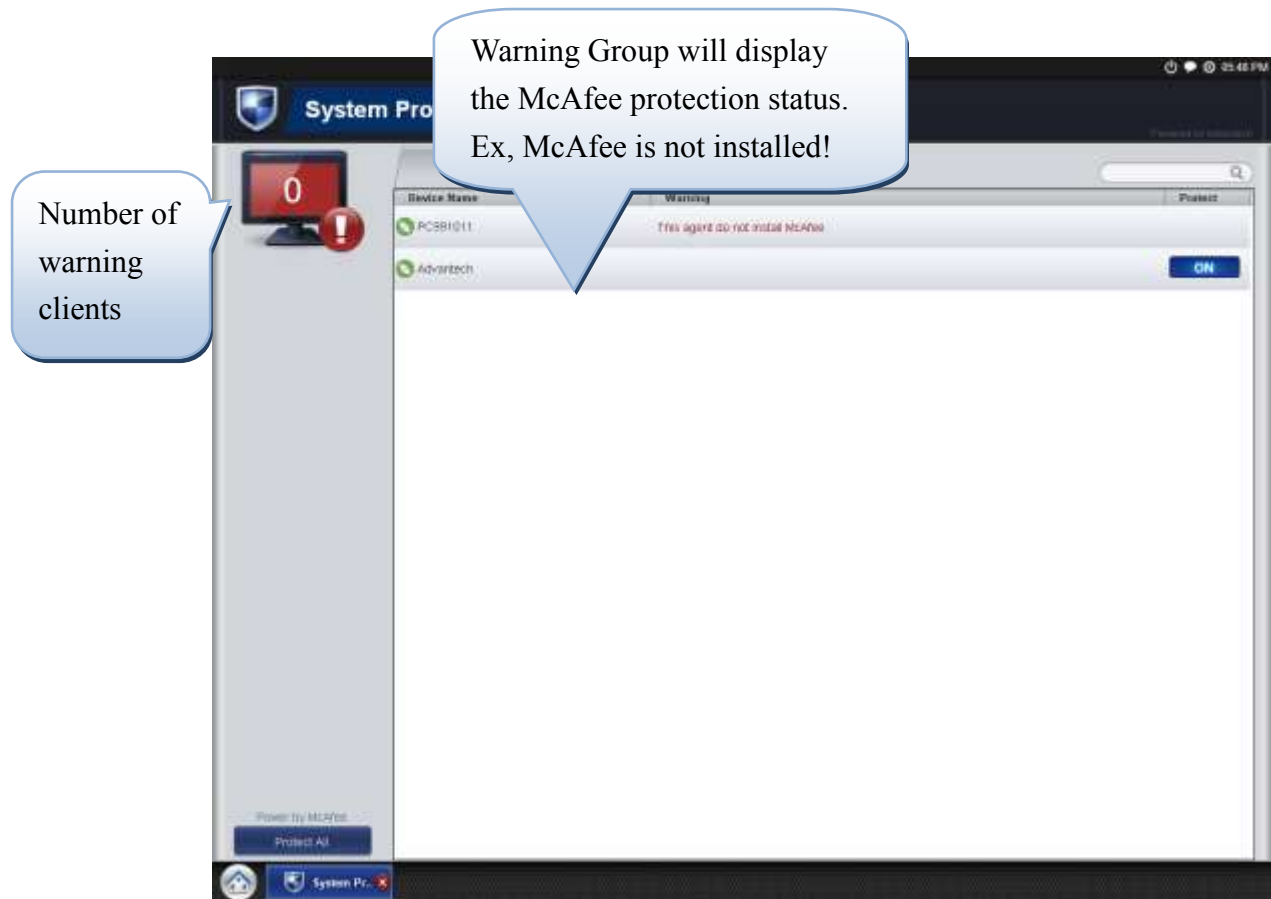
System Protection controls remote equipment, system protection and monitoring, and security. If a machine is threatened by a virus, the program will automatically detect and prevent intrusions.

*System Protection program integrates McAfee Embedded Security program which must be installed before use.

Click the **System Protection** icon to run the APP.

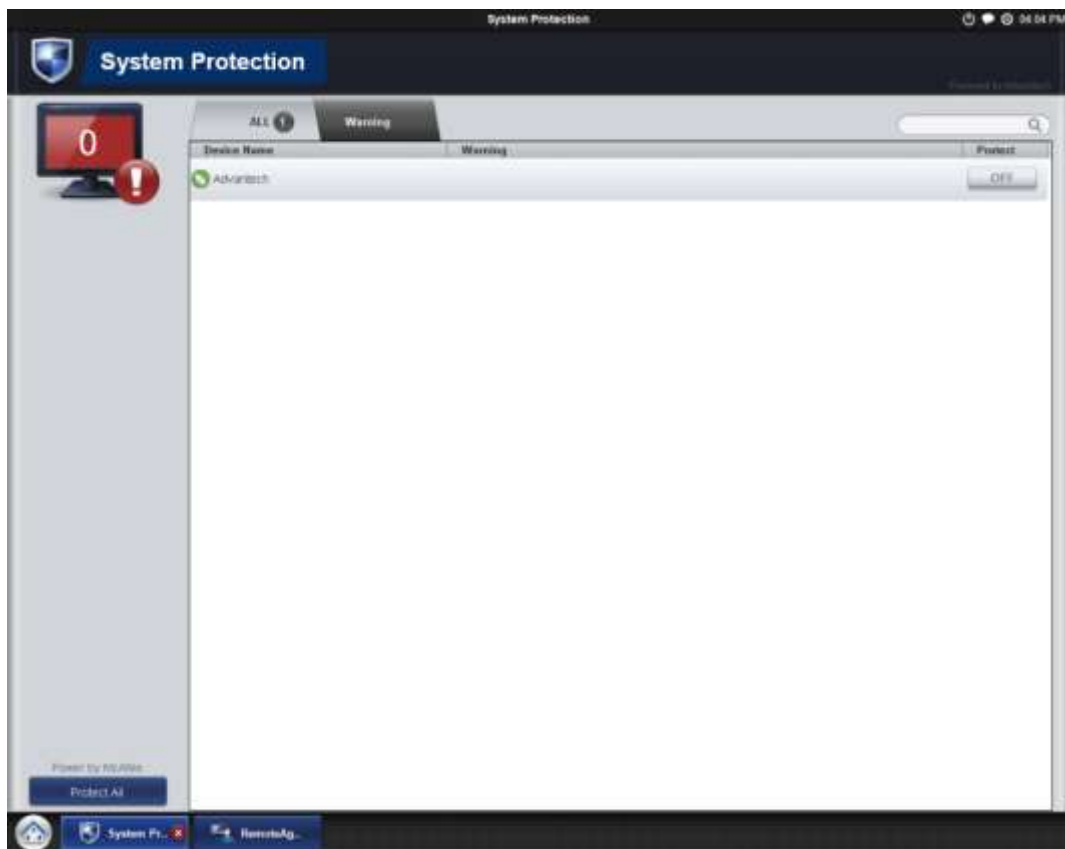


Below is the default System Protection user interface.

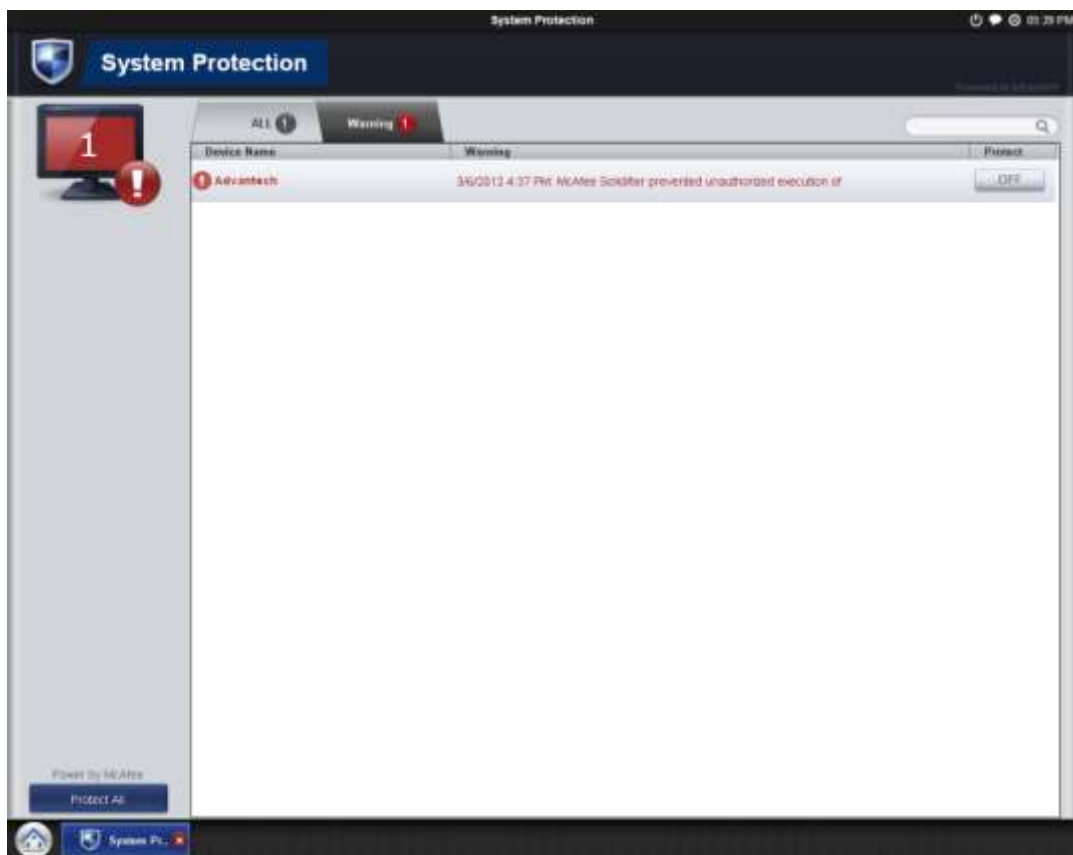


Protect All: Protect all connected devices

If the client connects to the server, it will show the following screen and status. For example, it shows the client name is "Advantech"; it is protected, and has no warnings.



If someone tries to execute, delete, or re-name files without permission, the client will send a report to the server, and you will get a warning message about system protection.



Furthermore, if you want to get details of previous warning messages, just click the client item.

