



Sentinel Network™

Free Trial Version

User Guide



Ridgetop Group, Inc.
3580 West Ina Road
Tucson, AZ 85741
Phone: (520) 742-3300
Fax: (520) 544-3180

The product described in this user guide is the free trial version of Sentinel Network, by Ridgetop Group

It is the policy of Ridgetop Group, Inc. (Ridgetop) to improve products as new technology, components, software, and firmware become available. Ridgetop, therefore, reserves the right to change specifications without prior notice.

All features, functions, and operations described herein may not be marketed by Ridgetop in all parts of the world. In some instances, photographs are of equipment prototypes. Therefore, before using this document, consult with your Ridgetop representative or Ridgetop office for information that is applicable and current.

To maintain the quality of our publications, we need your comments on the accuracy, clarity, organization, and value of this book.

Address correspondence to:

Manager, Technical Communication
Ridgetop Group Inc.
3580 West Ina Road
Tucson, AZ 85741 USA

Copyright ©2012
Ridgetop Group, Inc.
Tucson, Arizona USA
All Rights Reserved.

Rev041212

Table of Contents

1 About Sentinel Network	3
Technical Background	4
Switch Monitoring and Troubleshooting	4
Hardware Implementation	5
2 Getting Started.....	7
System Requirements	7
Installation Steps	7
3 Using Sentinel Network.....	9
Starting Sentinel Network.....	9
Running Network Discovery and Committing Assets.....	10
Discovering the Network.....	10
Committing Assets.....	12
Setting Up the Alerter to Send Email.....	13
Filtering Views	15
Flat vs. Subnet and Network Views	16
The Asset Properties and Real-Time Monitor Tabs	16
Using the HealthView Real-time Monitor.....	17
Performing Lightweight Monitoring.....	17
Performing Full Monitoring	18
Performing Real-time WMI Monitoring	20
Performing Real-time UPS Monitoring	21
Performing Background Monitoring.....	22
Adding or Removing Committed Assets	26
Adding a Device.....	26
Removing a Device	26
Monitoring Switches.....	27
4 Shutting Down and Uninstalling	29
Shutting Down Sentinel Network and the Virtual PC.....	29
Sentinel Network Uninstallation Steps.....	29
Virtual Machine Uninstallation Steps	29

Revision Record

Release	Date	Remarks
1	March 2, 2012	First issue, free trial version
2	April 12, 2012	Revisions in installation and uninstallation sections

Contact Information

Sales & Marketing

Phone: 520.742.3300

Email: sentinelnetwork@ridgetopgroup.com

Technical Support

Phone: 520.742.3300

Email: info@ridgetopgroup.com

Information Products Publishing

Contact: techcomm@ridgetopgroup.com

Corporate Location

Ridgetop Group, Inc.

3580 West Ina Road
Tucson, Arizona 85741

Phone: 520.742.3300

Fax: 520.544.3180

Website: www.ridgetopgroup.com

1 About Sentinel Network

Sentinel Network™ is an automated, web-based tool that continuously monitors the network, analyzes changes that affect performance, and reports problems via email messages to the IT network administrator for corrective action.

Sentinel Network provides customers with a powerful “net-centric” health management software platform solution, in a user-friendly graphical user interface (Figure 1).

The Sentinel Network tool performs¹:

- Accurate network discovery
- Network configuration monitoring
- Real-time health monitoring of workstations/servers
- Uninterruptible power supply (UPS) health monitoring based on load changes
- Background monitoring and data collection
- Switch monitoring and troubleshooting
- Real-time Windows management instrumentation (WMI) monitoring

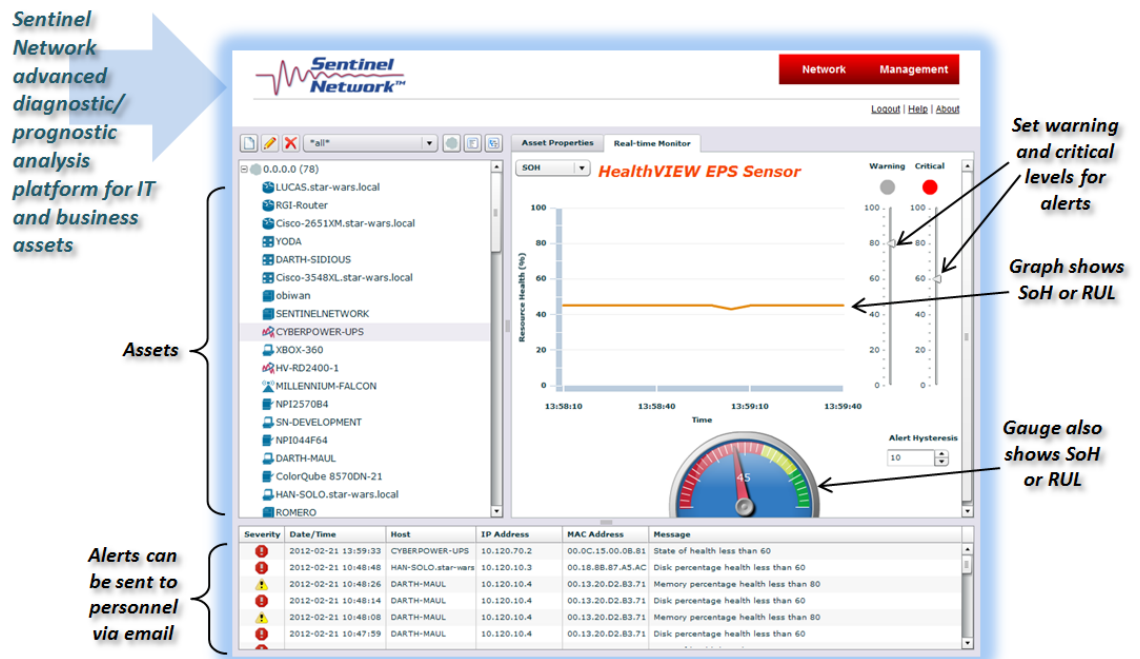


Figure 1: HealthVIEW Real-time Monitor tab in the Sentinel Network user interface

¹ Contact Ridgetop Group for information on how to enable UPS health monitoring and/or switch troubleshooting, which are not enabled by default in the free trial version.

Sentinel Network has been proven to customers as a viable solution for prognostics in IT networks.

Technical Background

The foundation of Sentinel Network is an extensible software platform that distributes sensor data collection, data fusion, reasoning, and presentation tasks. Sentinel Network also supports timely introduction and efficient software maintenance through its scalable design, enabling parallel development and support. Thus changes or the addition of more assets to the network are automatically supported. The distributed software architecture addresses these features with a modular web server design that separates the main client application from reasoner extensions and services that manage sensor data collection.

Sensor data are collected by leveraging the inherent simple network management protocol (SNMP) transport from the network's workstations, servers, switches, and UPS devices. The acquired sensor data are collected and stored to a central PHM database in Sentinel Network. The data are then processed using advanced diagnostic and prognostic reasoners, which process the multivariate sensor data to isolate the root cause of the fault condition and then estimate the remaining service life of the device being monitored.

For network devices, including UPS systems, this results in a remaining useful life (RUL) time estimate for impending failure and allows a technician to make the proper repairs or replacement to avoid downtime from equipment failure. The Sentinel Network PHM solution can be used to support a variety of sensor networks supporting critical systems, such as factory-floor automation cells, aircraft, automotive, and many other complex systems that cannot afford unscheduled maintenance due to system or subsystem malfunctions.

Critical networks can include routers, switches, servers, and potentially several thousand client nodes of varying type and function. The mission-critical components of the network are powered through UPSs. The UPS is responsible for providing clean, uninterrupted power for the connected network devices even during a power outage. The UPS is known to be a single point of failure for an IT network, as it powers the core of the network responsible for mission-critical systems. UPS devices have failure points similar to other power systems including batteries, capacitors, MOSFETs, and DC/AC inverter stages. The ability to predict the RUL of a UPS will improve the operational availability (Ao) and reliability of the network by reducing unplanned network downtime.

Switch Monitoring and Troubleshooting

During the initial network device discovery, an Alcatel series 9000 or series 6800 switch can be added via the switch monitoring configuration within Sentinel Network. Once this device is committed to Sentinel Network, an initial configuration from the device is taken as the default or baseline configuration from which to refer during switch monitoring. Switch configuration changes are detected when switch monitoring compares the new switch configuration file to the one

collected just after the initial discovery. When a change is detected, Sentinel Network alerts that the switch configuration has changed. Sentinel Network has the capability to help the network recover from a serious network failure when these configuration changes are detected. Sentinel Network utilizes an auxiliary connection to recover the managed switch through its serial port. This is done by reloading the managed device through the serial port. The user interface provides an automatic recovery option which connects to the managed device through the auxiliary connection and reloads the switch to the certified directory.

Hardware Implementation

The full version of Sentinel Network is also available as a hardware solution that can be deployed as a plug-in network device. This allows for full control of the target system. A one-rack unit (1RU) server was selected for the following reasons: size, energy consumption, and performance-to-cost ratio.

The Sentinel Network hardware implementation is shown in Figure 2. This 1RU box will mount in standard 19" server racks. The box is powered by a 1.8 GHz dual core Intel Atom processor, which provides sufficient processing power as well as low energy consumption. The baseline memory is 2 GB of DDR3 1333 MHz with an optional upgrade to 4 GB available. A 160 GB 7200 RPM hard drive also comes standard. Finally, a 250 W power supply powers the system. This hardware combination is available as a standard OEM package, making it a reliable system to deploy Sentinel Network.



Figure 2: Sentinel Network server appliance

2 Getting Started

System Requirements

The computer on which you run the Sentinel Network free trial version needs to have:

- Windows 7 Professional or Ultimate operating system
- Microsoft Windows Virtual PC software (free)
- 10 GB of free disk space
- 2048 MB RAM
- Network card, 10/100 Mbps minimum
- Monitor set at resolution of 1650 x 1050 or greater

Installation Steps

1. On the computer from which you want to run Sentinel Network, download and install the free Microsoft Windows Virtual PC application.
2. Obtain the virtual machine **sn2g-trial.zip** file and save it to the folder of your choice on the C-drive. For example, C:\sn2g-trial.
3. Extract the file into the same folder.
4. Double-click **sn2g.vmc**. If you see a dialog box that says the time stamp is inconsistent with current date, acknowledge it by clicking **OK**.
5. A Windows Security dialog box appears. Select **Use another account**.
6. In the login dialog box, enter **admin** for the username, and **password** for the password. The VM window appears.
7. Click the **Tools** menu and select **Settings**.
8. Click **Memory** in the left pane.
9. Enter **2048** in the memory setting box.
10. Click **Networking** in the left pane.
11. In the **Adapter 1** drop-down list box, select your network card.
12. Click **OK**.
13. Double-click the Sentinel Network 2G icon.
14. In the login dialog box, again enter **admin** for the username, and **password** for the password. Click **Login**.
15. Follow the steps under "Starting Sentinel Network," beginning on page 9.

3 Using Sentinel Network

Starting Sentinel Network

1. Double-click the Sentinel Network desktop icon. The browser Mozilla Firefox launches, and the login dialog box appears.
2. Log into Sentinel Network. The username is **admin** and the password is **password**.

The three-pane Sentinel Network main window appears (Figure 3). If you do not see the full window shown, simply click the red **Network** button to get there.

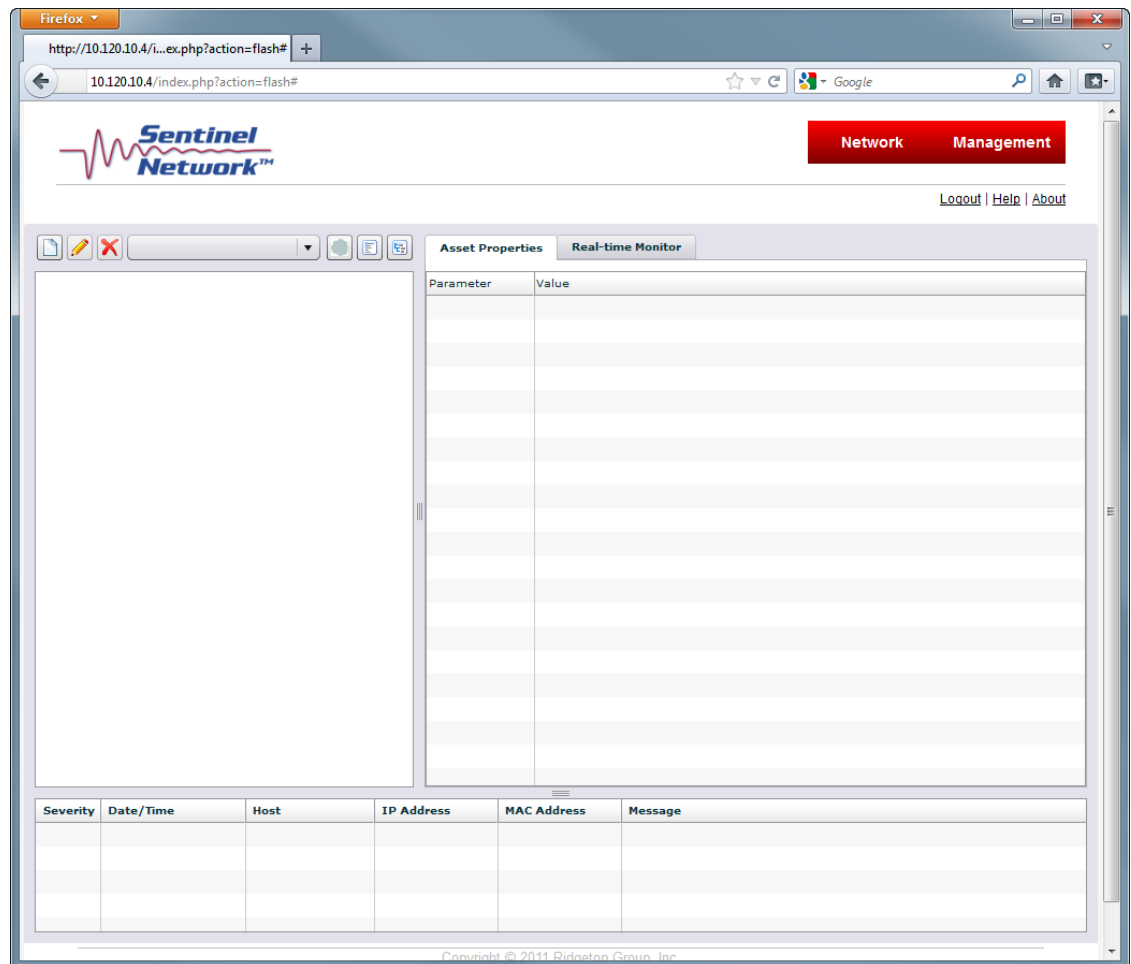


Figure 3: Sentinel Network, before network assets are discovered or committed

3. Follow the instructions under "Running Network Discovery and Committing Assets," starting on page 10.

Running Network Discovery and Committing Assets

The first time you use Sentinel Network, you must run discovery before any other features are available. Network discovery configures the database for the assets you will be analyzing.

Discovering the Network

1. Click the red **Management** tab at the top right of the window. Management opens to the first blue tab on the left, **Network Discovery** (Figure 4).

The screenshot shows the Sentinel Network Management interface. At the top right, there are two tabs: 'Network' (red) and 'Management' (red). Below this is a navigation bar with five blue tabs: 'Network Discovery', 'Alerter', 'Network Monitor', 'Background Monitor', and 'Switch Monitor'. The 'Network Discovery' tab is selected. The main content area contains the following configuration options:

- Discovery Type: Local Range SNMP
- IP Address Start: [] [] [] []
- SNMP Community String:
- Strategy: ping snmp
- SNMP Version: v1 v2 v3

At the bottom right, there are three buttons: 'Restore', 'Save', and 'Discover'.

Figure 4: Network Discovery tab in Management

2. Select the radio button for the Discovery Type you want to use – **Local**, **Range**, or **SNMP**, and follow these steps depending on which option you choose:

IMPORTANT: In steps a, b, and c, be sure to click **Save** before clicking **Discover** – if you do not click Save first, you will lose the information you just entered.

- a. **LOCAL:** If you select Local, only the networked devices that are on the same subnet as the machine on which you are running Sentinel Network will be detected. Enter your local IP address, or it will use the IP address of the network interface card you are using. Then select **Ping** and/or **SNMP** v1 or v2, depending on which version your devices use. Then click **Save**, and click **Discover**. Continue with step 4.
- b. **RANGE:** If you select Range, you can type in one or more ranges (start and end) of IP addresses that you know comprise the devices on

your network. Enter the first range, then to enter additional ranges, click **Add range**, which appears below the last range. You can also delete a range you have entered. After you have finished entering all ranges, select **Ping** and/or **SNMP v1** or **v2**, depending on which version your devices use. Then click **Save**, and click **Discover**. Continue with step 4.

- c. **SNMP:** If you select SNMP, an unrestricted search for all devices supporting SNMP devices on the network will be performed. SNMP will detect the greatest number of network devices while requiring the least amount of information. Enter a starting IP address, then select **SNMP v1** or **v2**, depending on which version your devices use. Click **Save**, then click **Discover**. Continue with step 4.

3. A dialog box warns that this process could take several minutes or longer, and asks if you are sure you want to proceed. Click **Yes** to continue.

The **Discovery in Process** dialog box provides feedback about the process. Eventually, the **Commit Assets** window appears in front of the Sentinel Network window, as shown in Figure 5.

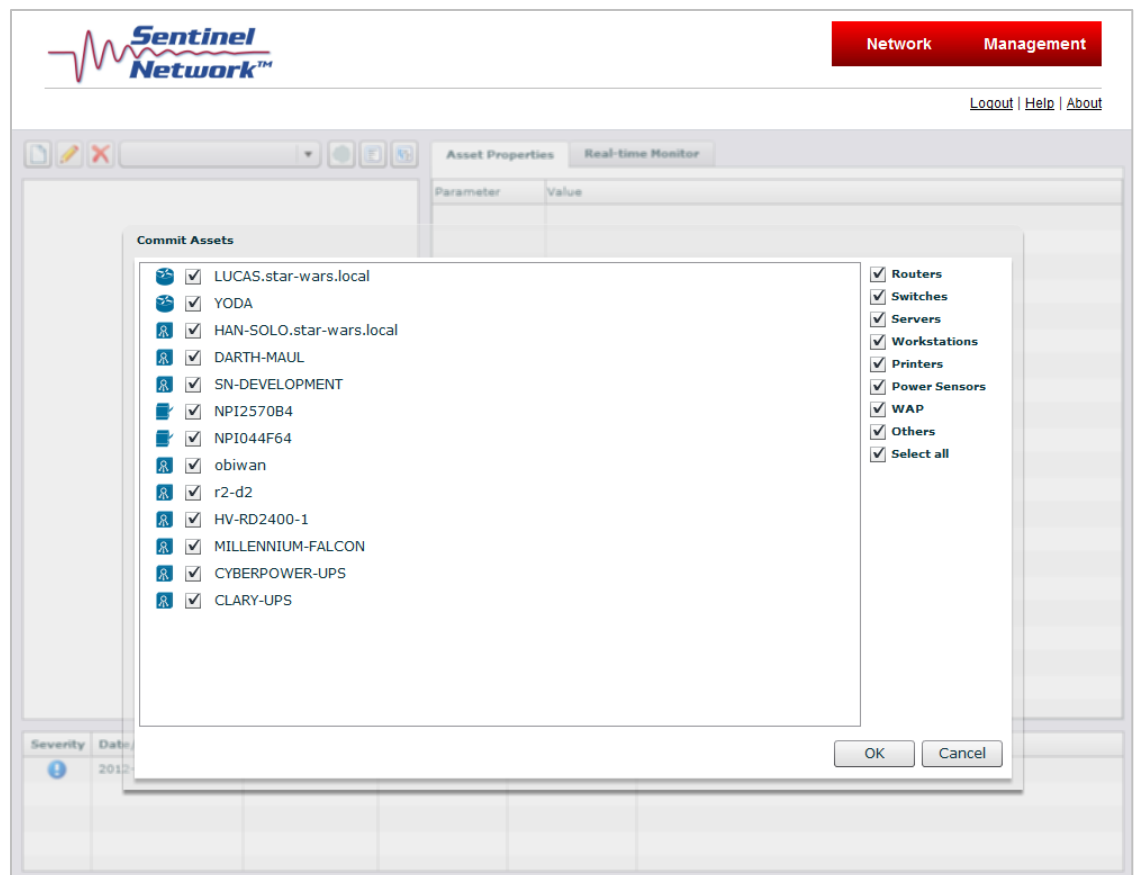


Figure 5: Commit Assets window

Committing Assets

4. At this point you can select which of the discovered assets you want to **commit** for monitoring by Sentinel Network. The check boxes on the right side of this dialog box (Figure 5), all of which are selected by default, enable you to keep or eliminate routers, switches, servers, workstations, printers, power sensors, WAP, or Others. The icons on the far left indicate the device type, although Discovery will typically not associate the correct icons with the devices during the first instance of discovery. Step 8 in this section provides the solution.

Note that Select all is a toggle switch that either selects all or clears all.

5. After you have ensured that the check boxes are selected for all the assets you want to commit, click **OK**.
6. A dialog box asks if you are sure. Click **Yes** to continue, or No to make changes to your selections.
7. In the main window, you will see at top left the discovered assets tree, shown as **0.0.0.0 (n)**, where n represents the number of assets committed. Click the **plus sign** next to this to reveal all the discovered assets that have been committed. Now the asset list will look similar to that shown in Figure 6.

Also notice that the first two alerts appear in the bottom pane, to announce discovery started and assets have been committed.

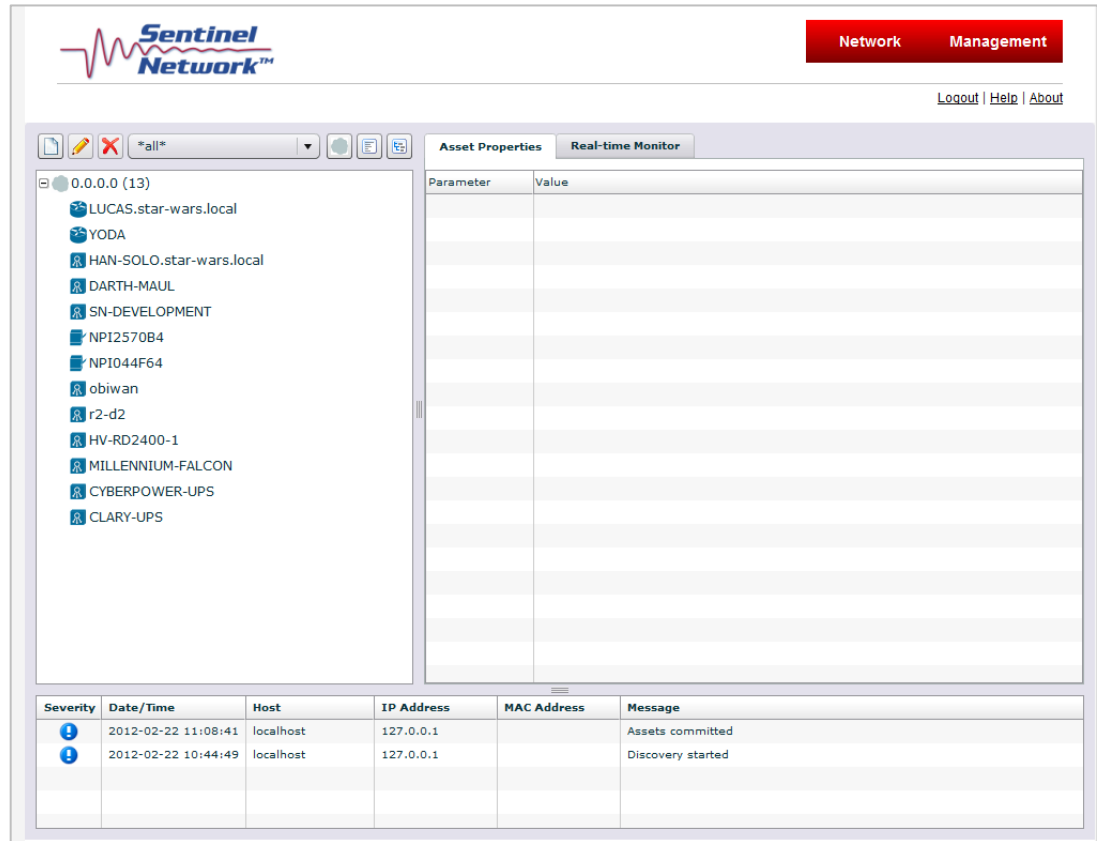


Figure 6: The discovered assets tree

- Open **translate.sed** from this path on the virtual machine: **C:\ws_app\discovery**. Use the examples provided in that file to set up your device type associations and/or delete extra IP addresses associated with certain devices. Then rerun Discovery by following the steps under "Running Network Discovery and Committing Assets," starting on page 10, to make your new graphic device type associations appear.

Setting Up the Alerter to Send Email

The settings for the Alerter dictate who will receive which types of alerts via email while Sentinel Network is running. These alerts will be the same ones that appear in the Alerter pane.

You can choose which data you want to appear in the email – the device's MAC address, IP address, Host, Level, Date, Time, and/or Event.

- Click the red **Management** tab.
- Click the blue **Alerter** tab.
- Select the **On** check box if you would like someone to receive alerts about the network devices' state of health (Figure 7).

The screenshot shows the Sentinel Network Management web interface. At the top right, there is a red 'Network Management' button. Below it are links for 'Logout', 'Help', and 'About'. A navigation bar contains five tabs: 'Network Discovery', 'Alerter' (which is selected), 'Network Monitor', 'Background Monitor', and 'Switch Monitor'. The main content area is titled 'Email' and contains the following configuration options:

- An 'Email' section with a checked checkbox labeled 'On'.
- An 'Email Recipients' section with the instruction '(separate with commas)'. It has three input fields:
 - Informational:
 - Warning:
 - Critical:
- An 'Email Contents' section with seven checked checkboxes: 'MAC', 'IP', 'HOST', 'Level', 'Date', 'Time', and 'Event'.

At the bottom of the configuration area, there are three buttons: 'Alerter Log', 'Restore', and 'Save'.

Figure 7: Setting the Alerter to send email

4. Enter at least one **email address** into the Informational, Warning, and/or Critical fields, depending on which types of alerts you want them to receive. You can separate additional email addresses with commas.

Note: Although there is no native text message support, you can enter email-to-text addresses, for example: 5201234567@att.txt.net

Informational alerts pertain to such things as lightweight monitoring starting and stopping, discover starting and stopping, full monitoring starting and stopping, and switch monitoring.

Warning alerts are generated when a device's health falls below the warning level (80% by default).

Critical alerts are generated when a device's health falls below the critical level (60% by default).

5. Select the check boxes for the type of information you would like included in each email message – MAC address, IP address, Host, Level, Date, Time, and/or Event.
6. Click **Save**.
7. In addition to configuring Sentinel Network for email generation, it is also necessary to modify the file **C:\PHP5\php.ini**. Open this file with your favorite text editor and search for **[mail function]**. The following should be displayed:

```
[mail function]
; For Win32 only.
SMTP = localhost
```


SMTP port = 25

8. Replace **localhost** with the name of your mail server, for example, mail.domain.com.
9. You must also restart Apache for this change to take effect. To do this, click **Start > Programs > Apache HTTP Server 2.2 > Control Apache Server > Restart**.

Filtering Views

Sentinel Network allows you to create custom views of your network assets by filtering them by type.

1. In the upper left corner, click the **Add View** icon to the left of the pencil (Edit view) icon. A window appears that is very similar to the commit assets window (Figure 8).

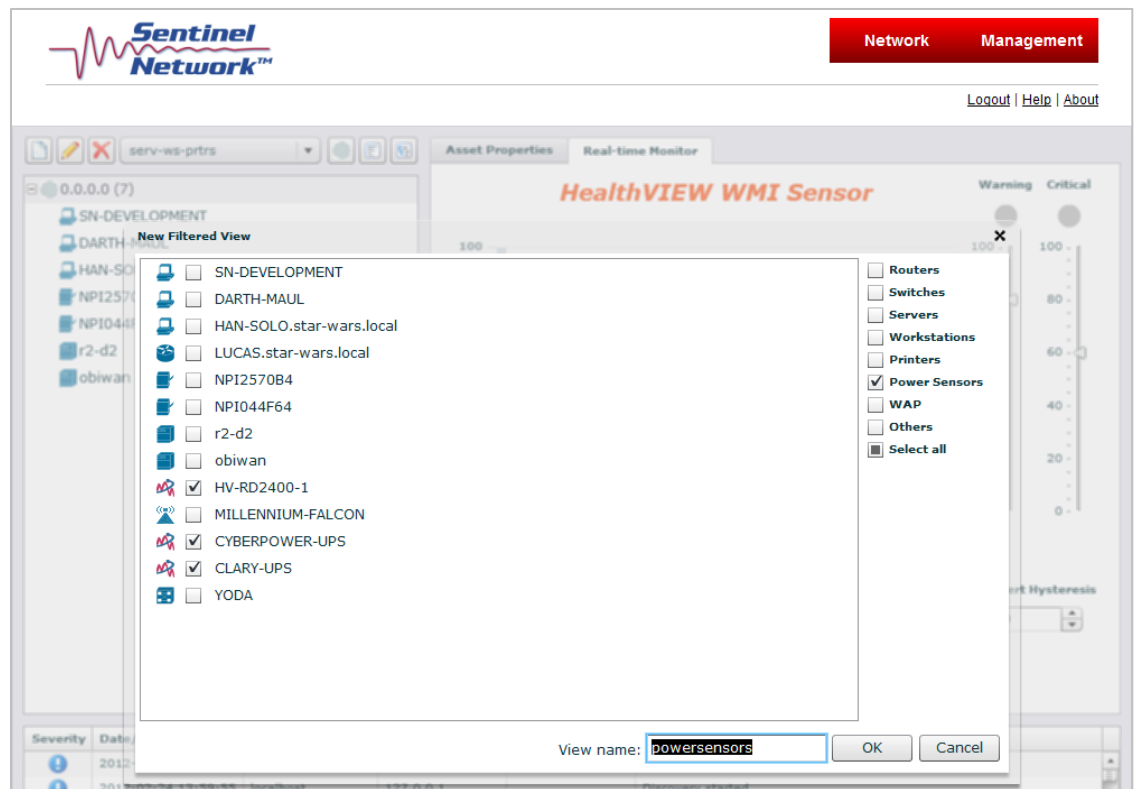


Figure 8: Filtering to view power sensors only

2. Clear the check boxes for the types of assets you don't want to see in this view, and leave one or more items checked, such as power sensors (as shown in Figure 8), or servers and workstations.

Note that Select all is a toggle switch that either selects all or clears all.

3. In the **View name** field at the bottom, give this view a representative name and click **OK**. Now this view appears in the drop-down list box to the right of the red X button, where you can select this or other views.

4. You can also modify any existing views by selecting the view from the list box then clicking the **Edit view** (pencil) icon. The window showing the filter appears, and you can change which items are checked, rename the view, and click **OK**.
5. To delete a filtered view, make sure it is selected from the list box, then click the **Delete view** (red X) button, and click **OK**.

Note: The *All* view cannot be deleted.

Flat vs. Subnet and Network Views

The three icons to the right of the View drop-down list box offer additional ways to view the network assets. The first one, which looks like a grey circle, is called the **Flat view**. This is the default view that shows all assets in one vertical column.

Click the **Subnet view** button to its right, and the assets are now positioned in relation to the subnet on which they are found (Figure 9). If this discovery was SNMP-based, some additional subnets may be found.

If you click the **Network view** button to the right of the Subnet view button, you will see assets positioned in relation to their hierarchy in the network.

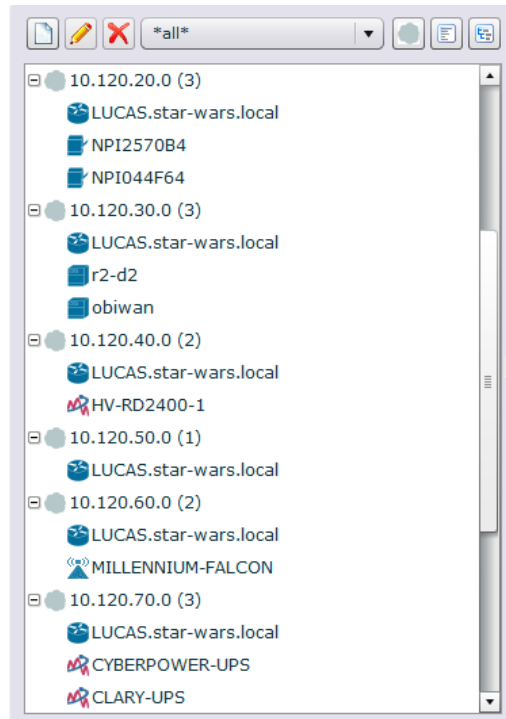


Figure 9: A subnet view

The Asset Properties and Real-Time Monitor Tabs

When you click a network asset in the left pane, in the right pane you will see the Asset Properties tab populated, and for some device types, the Real-time Monitor tab also appears.

Asset Properties shows the parameters of that asset that are available via SNMP: the hardware name, system name, ID, and properties about the network interface.

Using the HealthView Real-time Monitor

Certain types of assets can be monitored in the HealthView Real-time Monitor, such as servers and workstations with a Windows operating system. The real-time monitor view is called **HealthView**. Several types of monitoring are described in this section:

- Lightweight monitoring (page 17)
- Full monitoring (page 18)
- Real-time WMI monitoring (page 20)
- Background monitoring (page 22)

Note: All monitoring instructions assume that you have already discovered and committed your assets, as explained in "Running Network Discovery and Committing Assets," starting on page 10.

Performing Lightweight Monitoring

Lightweight monitoring is a way to detect when devices or assets on your network have "disappeared." It is a very fast process – you will immediately recognize when a device has gone off the network. To see how lightweight monitoring works, follow the steps in this section.

1. Disconnect one workstation from your network.
2. Click the red **Management** tab.
3. Click the center blue **Network Monitor** tab.
4. Select the **On** check box for Lightweight Monitor (Figure 10).

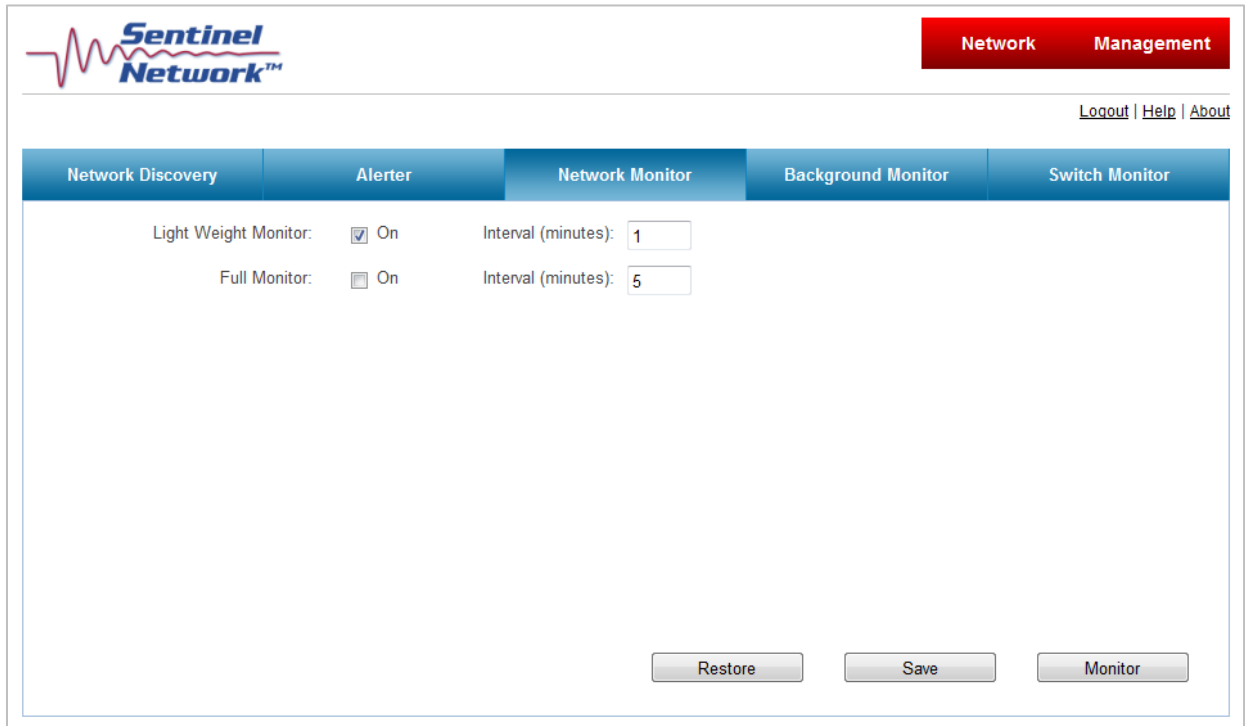


Figure 10: Lightweight monitoring window

5. Set the interval to **1** minute.
6. Click **Save** to save those settings.
7. Click the **Monitor** button.
8. Now click the red **Network** tab. In the bottom pane you will see that an alert has been generated, indicating that Lightweight monitoring has started, and another indicating it has completed.

Lightweight monitoring sends a ping to all the assets you've committed to the database. In addition to the alerts that monitoring has started and completed, because you have disconnected a workstation, you will soon see the alert "Committed asset unresponsive." It shows the MAC address and the IP address of that asset.

9. Reconnect the disconnected workstation. Lightweight monitoring will continue to execute, but will only produce informational alerts.
10. To stop lightweight monitoring, click the red **Management** tab, click the blue **Network Monitor** tab, and click **Stop Monitor**.

Note: The **Restore** button resets the default settings in Network Monitor.

Performing Full Monitoring

Full monitoring consists of a complete rediscovery of your network, with a comparison to the baseline network discovery. It takes significantly longer than lightweight monitoring. It is recommended to perform it once a day or once an hour, depending on the size of your network.

1. Click the red **Management** tab.
2. Click the blue **Network Monitor** tab.
3. Select the **On** check box for **Full Monitor** (refer to Figure 10) and clear the check box for lightweight monitoring.
4. Set the interval (in minutes). To determine the recommended minimum interval for full monitoring that will not result in an overlap, follow these guidelines:

Nodes	Full Monitoring Interval
<10	5 minutes
10 to 49	10 minutes
50 to 99	30 minutes
100 to 499	120 minutes
500 to 999	720 minutes
1000+	1440 minutes

5. Click **Save**.
6. Click **Monitor**.
7. Now click the red **Network** tab. Momentarily, in the bottom pane you will see that alerts have been generated, indicating that Discovery has started and assets have been committed. You will soon see the alert that full monitoring has started.
8. You can test monitoring by connecting or disconnecting a device from the network temporarily by turning off a port to a device and then turning the port back on, or by powering the device off and on again.

If you remove a device in this way, you will see the alert "Committed asset unresponsive." This will also generate an email alert, if you have enabled email alerting (see "Setting Up the Alerter to Send Email," page 13).

If you add a device, you will see the alert "New asset discovered." Right-click the device's alert in the Alerter pane and select **Add asset**. Click **Yes** when a dialog box asks if you are sure. This commits the asset to the database, and you will then see it appear in the left pane.

You can also remove a device that has generated an alert by right-clicking its alert and selecting **Remove asset**. Click **Yes** when a dialog box asks if you are sure. The asset then disappears from the left pane.

9. To stop full monitoring, go back to the red **Management** tab, click the blue **Network Monitor** tab, and click **Stop Monitor**.

Note: The Restore button resets the default settings in Network Monitor.

Performing Real-time WMI Monitoring

In this section you will learn how to perform foreground monitoring of Windows Management Instrumentation (WMI) for workstations and servers.

1. Click the red **Network** tab.
2. In the left pane, click a workstation or server you want to monitor.
3. Click the **Real-time Monitor** tab. This is showing foreground WMI monitoring. Note that the drop-down menu in the upper left corner allows you to monitor and view **CPU**, **Disk**, or **Memory** in real time (Figure 11).

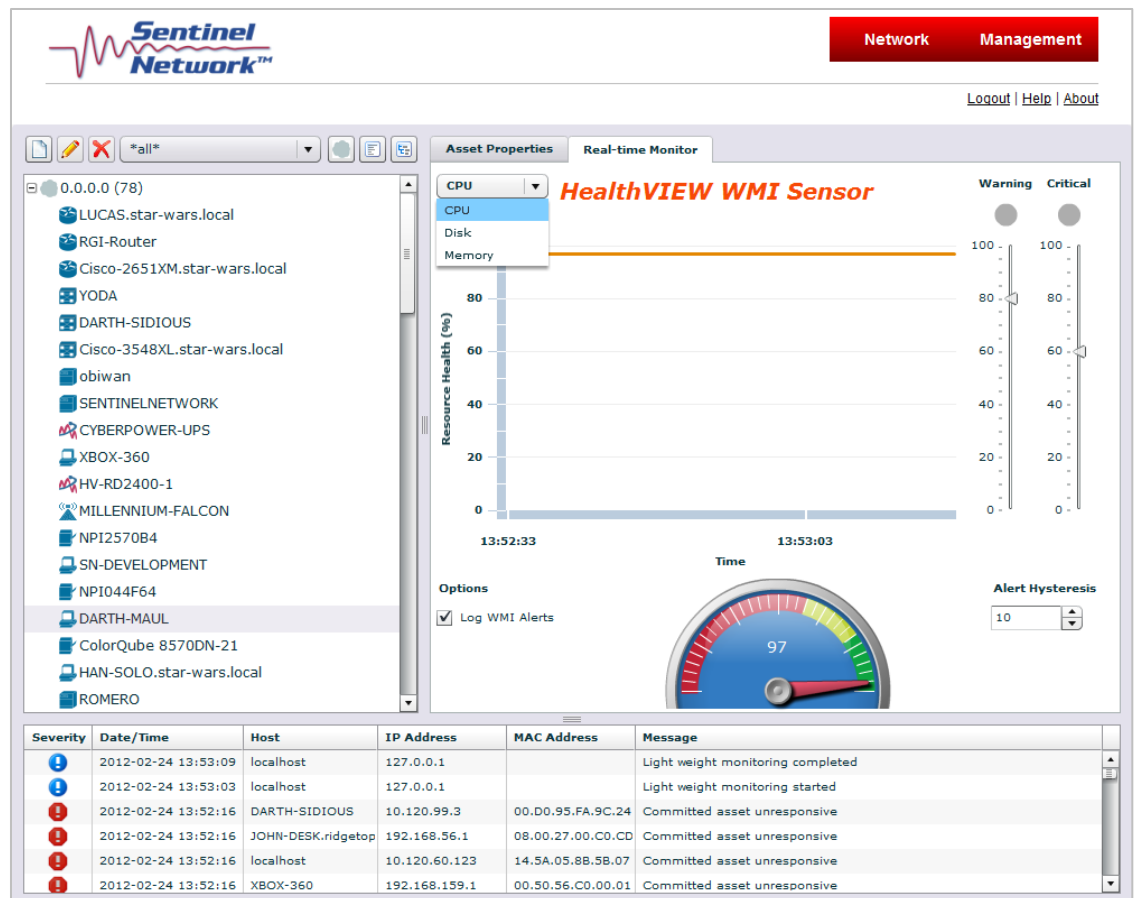


Figure 11: The CPU, Disk, or Memory menu in Real-time Monitor

4. Make sure that **CPU** is selected on the drop-down menu. This view shows in a graph the workstation's CPU health or how much "life" is remaining, as a percentage.

The resource health is also displayed in the "fuel gauge" at the bottom of the window, both numerically and visually by green, yellow, and red zones. Green indicates good health, yellow indicates a warning, and red indicates a very "used" or critical state.

Make sure the check box for **Log WMI Alerts** is selected, to the left of the fuel gauge. This is important because in the event that the CPU health decreases below the warning or critical threshold levels, alerts will be generated in the Alerter pane. If you clear this check box, you will not receive any alerts.

If the CPU is not being used much, you should see high health values such as those shown in Figure 11.

Note: For each device that shows the HealthView Real-time Monitor tab, you can set the threshold at which you want to receive warning and critical alerts by dragging the Warning and Critical arrows on the right side of that pane up and down.

5. Now select the **Disk** space parameter from the drop-down menu. You will likely see the graph and gauge go lower, indicating how much disk space is remaining, possibly even generating an alert in the Alerter pane.
6. Now select the **Memory** parameter. The graph and gauge will change again. If you left the Log WMI Alerts option checked, and memory is below the threshold values set on the right side of the pane, you may receive an alert about the memory percentage health in the Alerter pane.

Performing Real-time UPS Monitoring

In this section you will learn how to perform foreground health monitoring of uninterruptable power supplies (UPSs). UPSs typically power the servers or critical components in your network's electric power system (EPS). Note that this version of Sentinel Network only supports CyberPower UPSs.

1. From the **Network** tab, in the left pane, click a CyberPower UPS that you have on your network.
2. Click the **Real-time Monitor tab** (Figure 12) to see foreground UPS monitoring. Note that the drop-down menu in the upper left corner allows you to monitor and view either **RUL** (remaining useful life) or **SOH** (state of health) in real time.

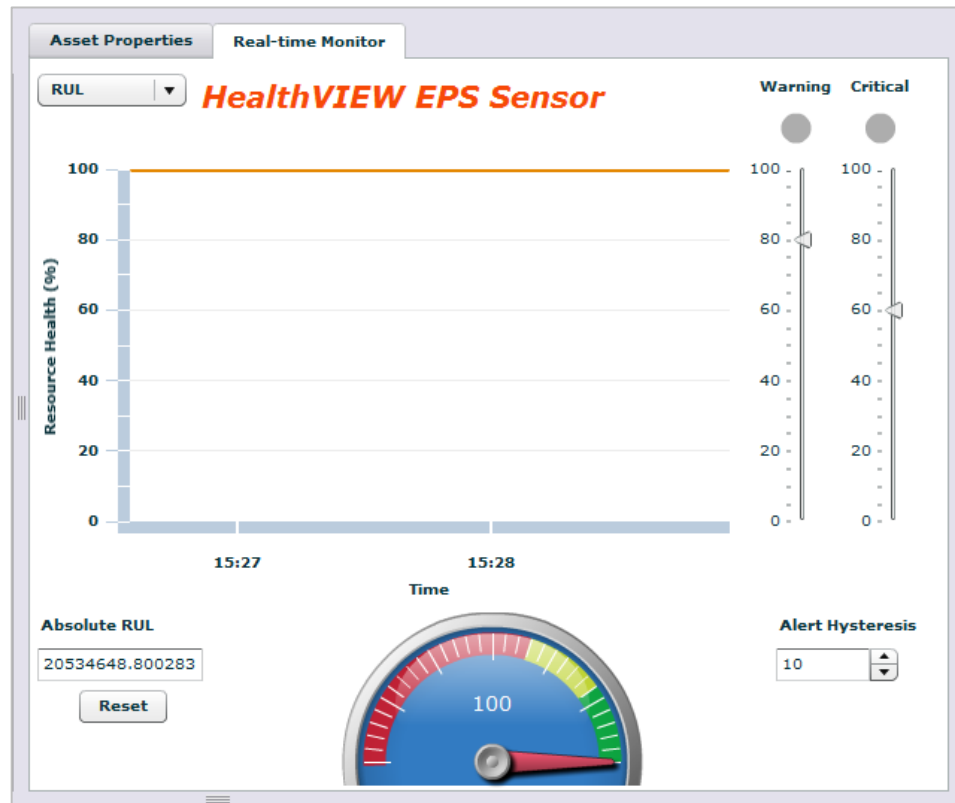


Figure 12: Real-time monitor of UPS remaining useful life

3. Make sure **RUL** is selected from the drop-down menu at top left. The real-time monitor displays the resource health in terms of a percentage on the left. It also shows a graphical display, and gives an absolute health value in the lower left corner. A numeric percentage and visual indicator are also supplied in the fuel gauge.

You can demonstrate the operation of this UPS monitoring feature by putting an increasing load on the UPS. It might not be enough to change the graph, but you should start to see a change in the **Absolute RUL** health value.

You will eventually see a drop in the device's overall health reading based on the algorithm used to compute it. The system model used for the UPS health feature is based on the two-year lifetime of a typical UPS product. Based on the load, we can compute the health value.

Performing Background Monitoring

Background monitoring is similar to foreground monitoring with the exception that it logs the resource health for CPU, Disk, and Memory at a user-defined interval for workstations and servers. It can also log UPS state of health, percent RUL, and absolute RUL. It runs on a separate web page.

1. Click the red **Network** tab.
2. Click a workstation or server to monitor.
3. Click the Asset Properties tab.

4. Make a note of the workstation's IP address, which shows on the Asset Properties tab.
5. Click the red **Management** tab.
6. Click the blue **Background Monitor** tab. The window shown in Figure 13 appears.

The screenshot shows the Sentinel Network web interface. At the top left is the Sentinel Network logo. At the top right, there are two red tabs: 'Network' and 'Management'. Below these, there are links for 'Logout | Help | About'. A navigation bar contains five blue tabs: 'Network Discovery', 'Alerter', 'Network Monitor', 'Background Monitor' (which is selected), and 'Switch Monitor'. The main content area has four input fields with labels: 'Interval (minutes):' with the value '1', 'Warning threshold (percent):' with '80', 'Critical threshold (percent):' with '60', and 'Hysteresis (percent):' with '10'. To the right of these fields is a blue link labeled 'Add New Device'. At the bottom of the interface are four buttons: 'Background Log', 'Restore', 'Save', and 'Stop'.

Figure 13: Background Monitor tab

7. Set the **Interval** to **1** minute, for demonstration purposes. Ordinarily, you might want to run background monitoring once an hour or once every few hours, depending on the device.

You can change any of the remaining three fields – warning and critical threshold percentages, and hysteresis percent – or keep the default settings.

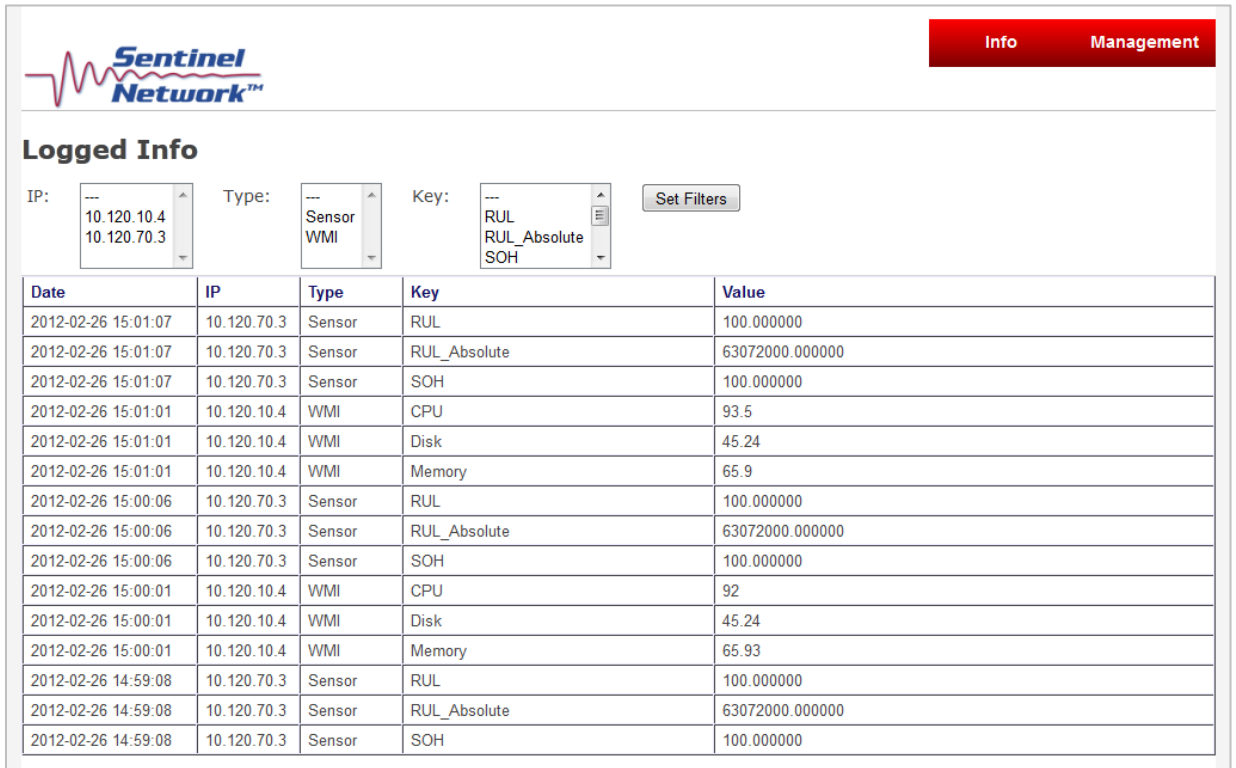
8. Click **Add New Device**, on the right.
9. In the **IP address** field that appears (Figure 14), enter the workstation, server, or UPS IP address.



Network Discovery	Alerter	Network Monitor	Background Monitor	Switch Monitor
Interval (minutes): <input type="text" value="1"/>				
Warning threshold (percent): <input type="text" value="80"/>				
Critical threshold (percent): <input type="text" value="60"/>				
Hysteresis (percent): <input type="text" value="10"/>				
IP <input type="text"/> <input type="checkbox"/> Sensor <input type="checkbox"/> WMI				
<input type="button" value="Background Log"/> <input type="button" value="Restore"/> <input type="button" value="Save"/> <input type="button" value="Stop"/>				

Figure 14: Adding devices for background monitoring

10. Select the check box for **WMI** for workstations and servers. Select the check box for **Sensor** if you want to monitor a UPS.
11. Click **Save**. The Add New Device option appears again, so you have the option of adding more devices.
12. After you are finished adding IP addresses, click **Start**.
13. Click the **Background Log** button. A new Logged Info window appears (Figure 15) on a separate web page.



Date	IP	Type	Key	Value
2012-02-26 15:01:07	10.120.70.3	Sensor	RUL	100.000000
2012-02-26 15:01:07	10.120.70.3	Sensor	RUL_Absolute	63072000.000000
2012-02-26 15:01:07	10.120.70.3	Sensor	SOH	100.000000
2012-02-26 15:01:01	10.120.10.4	WMI	CPU	93.5
2012-02-26 15:01:01	10.120.10.4	WMI	Disk	45.24
2012-02-26 15:01:01	10.120.10.4	WMI	Memory	65.9
2012-02-26 15:00:06	10.120.70.3	Sensor	RUL	100.000000
2012-02-26 15:00:06	10.120.70.3	Sensor	RUL_Absolute	63072000.000000
2012-02-26 15:00:06	10.120.70.3	Sensor	SOH	100.000000
2012-02-26 15:00:01	10.120.10.4	WMI	CPU	92
2012-02-26 15:00:01	10.120.10.4	WMI	Disk	45.24
2012-02-26 15:00:01	10.120.10.4	WMI	Memory	65.93
2012-02-26 14:59:08	10.120.70.3	Sensor	RUL	100.000000
2012-02-26 14:59:08	10.120.70.3	Sensor	RUL_Absolute	63072000.000000
2012-02-26 14:59:08	10.120.70.3	Sensor	SOH	100.000000

Figure 15: Background monitoring Logged Info window

You will see that some data have already been generated in the Logged Info window. These values will change every 1 minute.

Note: If there are hyperlinked numbers at the bottom of the window (not shown in Figure 15), they will take you to the pages of values generated. Each time the number of responses exceeds 15, a new page is created.

14. In the Logged Info window, in the upper left **IP** list box, click the IP address of the workstation/server you added.
15. For **Type**, click **WMI**.
16. For **Key**, scroll down and select **CPU, Disk, and Memory** (hold down the **Ctrl** button to select more than one item).
17. Click the **Set Filters** button. The window shown in Figure 16 appears. The values in the far right column indicate resource health percentages.
18. Press **F5** to refresh the window.

Logged Info

IP: 10.120.10.4
 Type: Sensor
 Subtype: WMI
 Key: SOH, CPU, Disk, Memory

Date	IP	Type	Key	Value
2012-02-26 15:23:01	10.120.10.4	WMI	CPU	93.5
2012-02-26 15:23:01	10.120.10.4	WMI	Disk	45.24
2012-02-26 15:23:01	10.120.10.4	WMI	Memory	65.92
2012-02-26 15:22:01	10.120.10.4	WMI	CPU	93
2012-02-26 15:22:01	10.120.10.4	WMI	Disk	45.24
2012-02-26 15:22:01	10.120.10.4	WMI	Memory	65.92
2012-02-26 15:21:01	10.120.10.4	WMI	CPU	93
2012-02-26 15:21:01	10.120.10.4	WMI	Disk	45.24
2012-02-26 15:21:01	10.120.10.4	WMI	Memory	65.92
2012-02-26 15:20:01	10.120.10.4	WMI	CPU	93
2012-02-26 15:20:01	10.120.10.4	WMI	Disk	45.24
2012-02-26 15:20:01	10.120.10.4	WMI	Memory	65.92
2012-02-26 15:19:01	10.120.10.4	WMI	CPU	93
2012-02-26 15:19:01	10.120.10.4	WMI	Disk	45.24
2012-02-26 15:19:01	10.120.10.4	WMI	Memory	65.92

1 2 3 4 5 Next

Figure 16: Logged WMI info for workstation/server – CPU, disk, and memory

When you are finished reviewing it, you can simply close that Firefox web page. Sentinel Network remains running on the original page.

Adding or Removing Committed Assets

Adding a Device

1. To add a new device to the committed assets list, connect the asset to the network, then follow the instructions under “Running Network Discovery and Committing Assets,” starting on page 10.

You will soon see the alert “New asset discovered.” This will also generate an email alert, if you have enabled email alerting (see “Setting Up the Alerter to Send Email,” page 13).

2. Right-click that alert and from the context menu that appears, select **Add asset**. Click **Yes** when a dialog box asks if you are sure. This commits the asset to the database. A new alert says “New committed asset.”

Removing a Device

1. You can remove an asset from the network by turning off a port to a device or by powering it off. You will soon see an alert that says “Committed asset unresponsive.” This will also generate an email alert, if you have enabled email alerting (see “Setting Up the Alerter to Send Email,” page 13).

- Right-click the alert and from the context menu that appears, select **Remove asset**. The asset will no longer be in the Sentinel Network database. Click **Yes** when a dialog box asks if you are sure. The asset then disappears from the left pane, and is removed from the database. A new alert says Committed asset removed.

Monitoring Switches

Switch monitoring is supported only for Alcatel 6800 and 9000 series switches in this trial version of Sentinel Network.

- Click the red **Management** tab.
- Click the blue **Switch Monitor** tab.
- Under **Switch FTP access**, enter the **IP address** for the switch you are going to be monitoring and troubleshooting (Figure 17).

The screenshot shows the Sentinel Network web interface. At the top right, there are two tabs: 'Network' (red) and 'Management' (red). Below them are links for 'Logout', 'Help', and 'About'. A navigation bar contains five tabs: 'Network Discovery', 'Alerter', 'Network Monitor', 'Background Monitor', and 'Switch Monitor' (highlighted in blue). The main content area is titled 'Switch Monitor' and contains the following form:

Switch FTP Access:

Host/IP:

Login:

Password:

Dump options:

Interval:

Remote file:

At the bottom of the form are four buttons: 'Restore', 'Save', 'Test connection', and 'Stop Monitor'.

Figure 17: Setting up switch monitoring

- Enter your **login** username (admin) and password (password).
- Under **Dump options**, enter the interval at which you want to retrieve the boot configuration, such as 1 (minute).
- For **Remote file**, enter the boot configuration file name, **boot cfg**, as shown in Figure 17.
- Click **Save**.
- Click **Test Connection**. The message "Connection test passed" should appear in the upper left area.

9. Click **Monitor**.
10. Click the red **Network** tab. Momentarily, you should see alerts that say switch monitoring started and switch monitoring completed. You might also see an alert that says switch configuration changed.

4 Shutting Down and Uninstalling

Shutting Down Sentinel Network and the Virtual PC

After running Sentinel Network, when you want the Virtual PC to be completely shut down and not running in the background:

1. Close the Sentinel Network window.
2. Click the **Ctrl+Alt+Del** menu in Virtual PC, and click **Shut Down**.
3. Select **Shut Down** again, and click **OK**.

Sentinel Network Uninstallation Steps

Your installation of Sentinel Network will expire 30 days from installation. However, should you wish to remove Sentinel Network before that, you need only delete the files by following these steps:

1. Click **Start > All Programs > Windows Virtual PC**.
2. Right-click **sn2g Applications**, and select **Delete** from the context menu.

Virtual Machine Uninstallation Steps

1. If the virtual machine is running, shut it down or turn it off.
2. If you want to delete the virtual hard disks, open the settings for the virtual machine and note the location of all virtual hard disks.
3. From the Virtual Machines folder, right-click the name of the virtual machine and then click **Delete**. The virtual machine is removed from the folder and the virtual machine (.vmcx) file is moved to the Recycle Bin.
4. Open Windows Explorer and browse to the location where the virtual machine files are stored. For example, the default location for virtual machine files is the following, where *username* is the name of your Windows 7 user account: **%systemdrive%\Users\username\AppData\Local\Microsoft\Windows Virtual PC\Virtual Machines**.
5. Look for and delete files that are named the same as the virtual machine and have the following extensions: .vmc, .vmc, .vpckbackup, .vsv, .vht, and .vud. You also can search for files with those extensions.
6. Empty the Recycle Bin.

