MINUTEMAN®
POWER TECHNOLOGIES
by Para Systems, Inc.

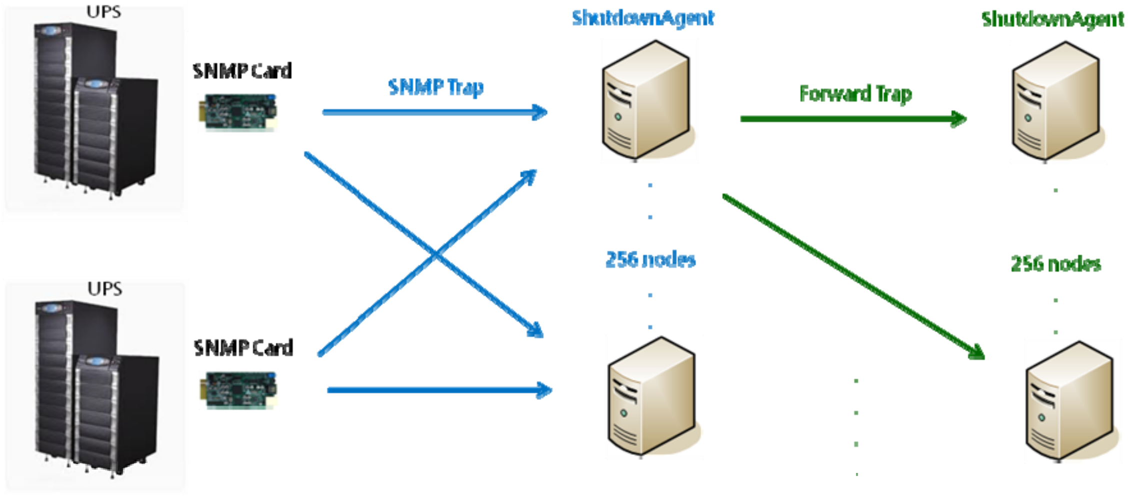
MM ShutdownAgent

User Manual

Contents

1. Overview

The MM ShutdownAgent software can protect the operating system during a power failure. Using a Web Browser, you can easily obtain the current UPS events, shutdown strategy and countdown information.



1.1 Features

1. Supports SNMPv1, SNMPv3 traps.
2. Supports SNMPv1, SNMPv3 server access for monitoring the ShutdownAgent status and configure the shutdown parameters.
3. Provides web interface through HTTP and HTTPS.
4. Provides batch configuration.
5. Can Forward SNMP traps to 255 servers.
6. Supports up to 32 trap sources for redundant (logical OR) and parallel (logical AND) application.
7. Provides console configuration for basic system parameters.
8. Supports Windows 32/64 bit programs.

1.2 OS Support

Windows XP-sp2, Vista, 7, 8
Windows 2003, 2008
Windows 2008 Server Core, Hyper-V 2008 R2
Linux OpenSUSE 11.4
Linux ubuntu 10.04
Linux Fedora 3.1.9
CentOS 5.8
VMWare ESXi 4.1, 5
Citrix XenServer 6.0.0
Linux KVM

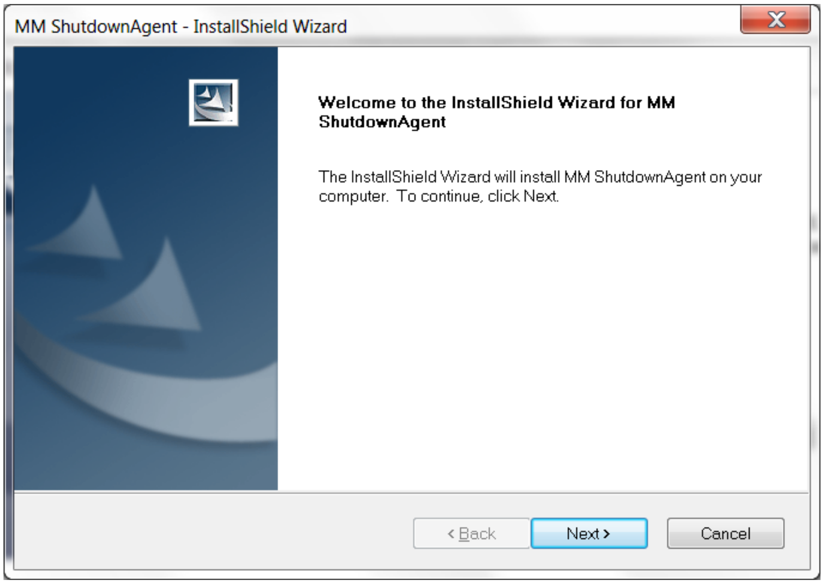
2. Installation / Uninstall

2.1 For Windows System

There are two setup programs: MM-ShutdownAgent-Setup(win32).exe and MM-ShutdownAgent-Setup(x64).exe. One is for 32 bit Windows operating system and the other one is for 64 bit Windows environment.

2.1.1 Installation Process

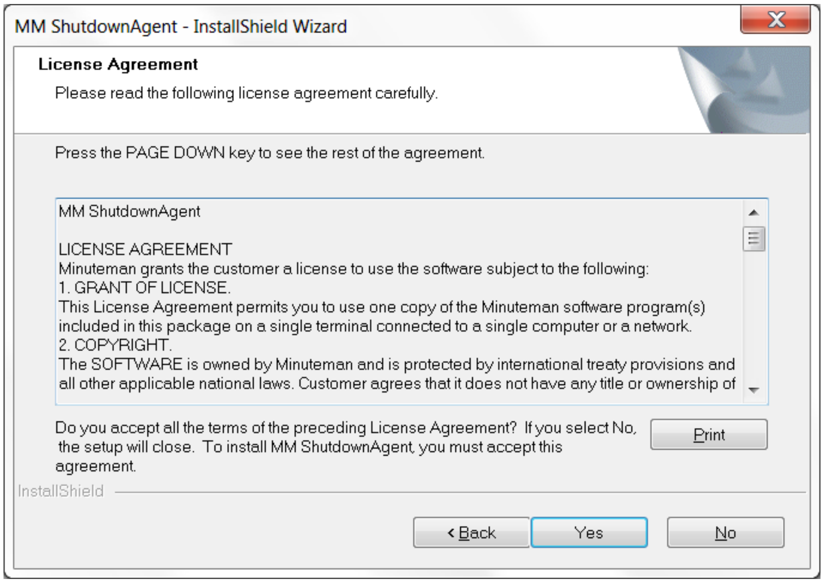
1. Execute the MM-ShutdownAgent-Setup (xxx).exe to run the setup program.
2. The welcome page will be displayed, press the “Next” button to continue with the installation.



Welcome to the InstallShield Wizard for MM ShutdownAgent

The InstallShield Wizard will install MM ShutdownAgent on your computer. To continue, click Next.

3. Press the “Yes” button to accept the license agreement and continue with the installation.



License Agreement

Please read the following license agreement carefully.

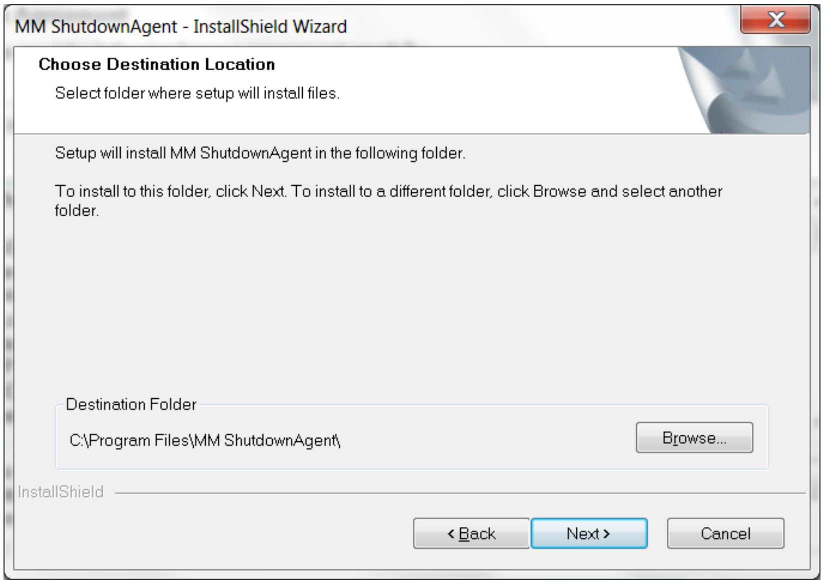
Press the PAGE DOWN key to see the rest of the agreement.

MM ShutdownAgent

LICENSE AGREEMENT
Minuteman grants the customer a license to use the software subject to the following:
1. GRANT OF LICENSE.
This License Agreement permits you to use one copy of the Minuteman software program(s) included in this package on a single terminal connected to a single computer or a network.
2. COPYRIGHT.
The SOFTWARE is owned by Minuteman and is protected by international treaty provisions and all other applicable national laws. Customer agrees that it does not have any title or ownership of

Do you accept all the terms of the preceding License Agreement? If you select No, the setup will close. To install MM ShutdownAgent, you must accept this agreement.

4. Select a different location by using the Browse button or press the “Next” button to install the software in the default location.


MM ShutdownAgent - InstallShield Wizard
Choose Destination Location
InstallShield
Browse...
< Back
Next >
Cancel

Select folder where setup will install files.

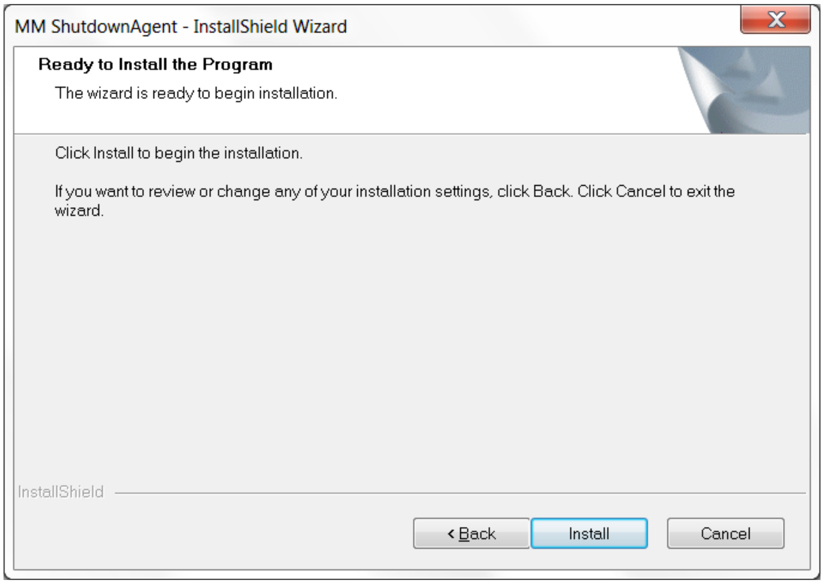
Setup will install MM ShutdownAgent in the following folder.

To install to this folder, click Next. To install to a different folder, click Browse and select another folder.

Destination Folder

C:\Program Files\MM ShutdownAgent\

5. Press the “Install” button to start installing the software to the designated location.

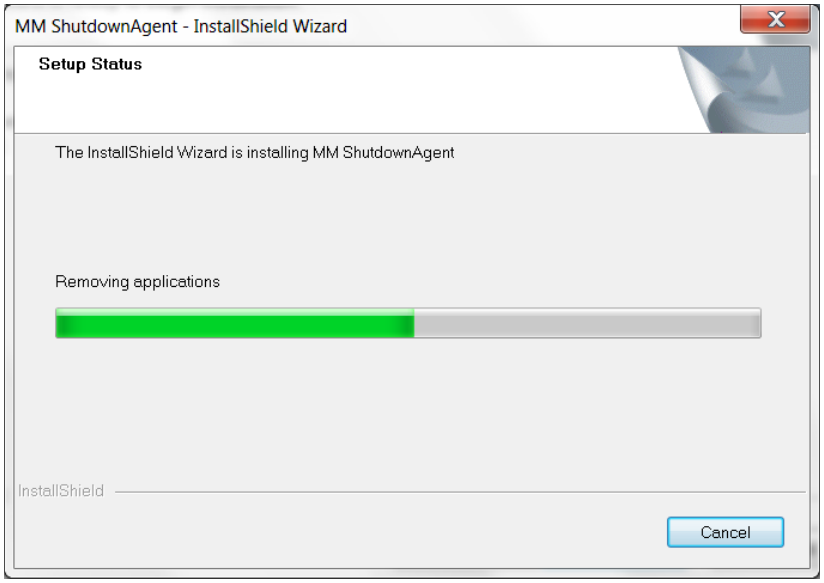

MM ShutdownAgent - InstallShield Wizard
Ready to Install the Program
InstallShield
< Back
Install
Cancel

The wizard is ready to begin installation.

Click Install to begin the installation.

If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.

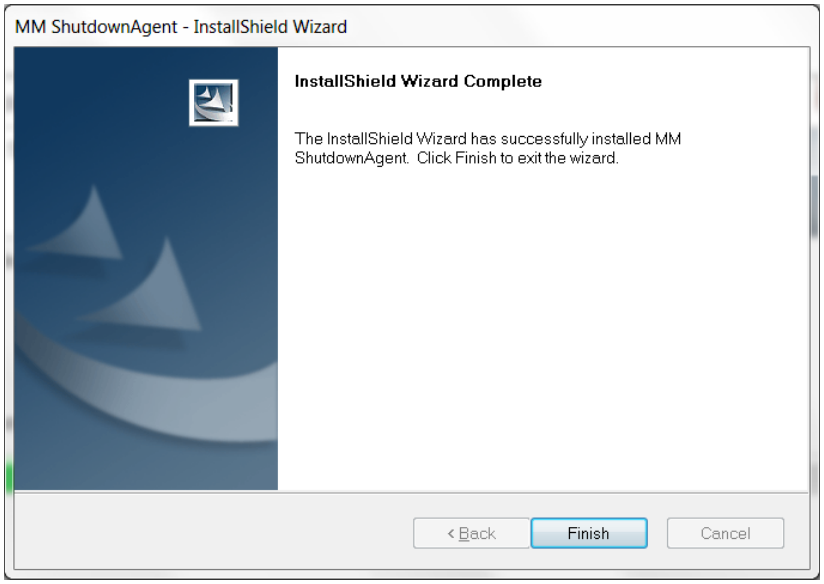
6. The Installation is in process.



The InstallShield Wizard is installing MM ShutdownAgent

Removing applications

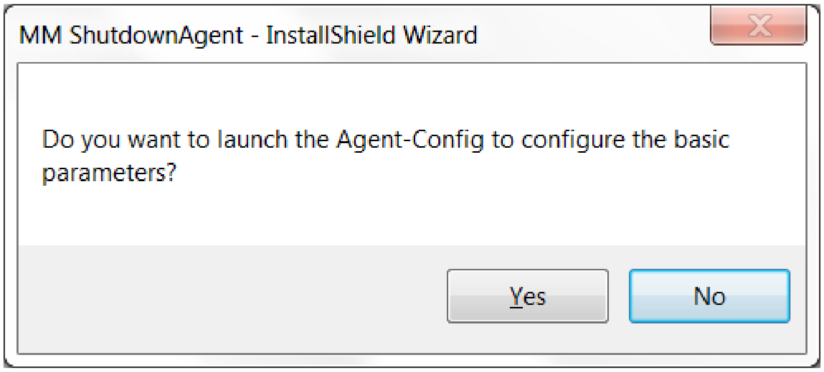
7. After the installation is finished, press the “Finish” button to exit the installation process.



InstallShield Wizard Complete

The InstallShield Wizard has successfully installed MM ShutdownAgent. Click Finish to exit the wizard.

8. After finishing the installation, the ShutdownAgent will automatically start the service program and add an icon to indicate its status in the Task Bar / Start Menu. Meanwhile, a dialog box will pop up to ask if you want to launch the Agent-Config application to configure the basic parameters. Press the Yes button to launch the Agent-Config to configure in the Shell mode (see Chapter 3). Or press the No button to finish the installation and then open the Start Menu and find the MM ShutdownAgent folder to either use the Console Configure or the Web Monitor to configure the parameters for the software.



MM ShutdownAgent - InstallShield Wizard

Do you want to launch the Agent-Config to configure the basic parameters?

The **ShutdownAgent** software is comprised of two modules:

A **Service** module (**Shutdown-Agent Service: Agent-Service.exe**), which runs in the background as a Service and listens for the SNMP trap from the source IP addresses.

A **Status** module (**Agent-Status.exe**), which enables you to control and configure the software through drop down menus and dialog boxes. It also allows you to launch the web browser and login automatically to monitor, configure and control the software.

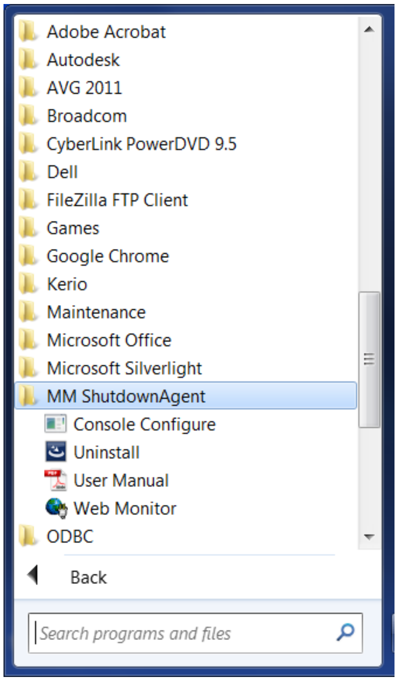
After finishing the installation, the setup program will create a MM ShutdownAgent association with the following shortcuts:

Console Configure: Launches the Agent-Config.exe to configure the basic parameters.

Uninstall: Removes the MM ShutdownAgent. The configuration data will still be kept in the installed directory.

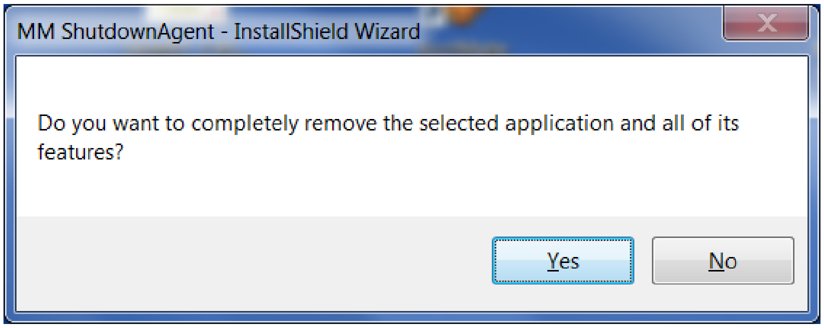
User Manual: The user manual is in PDF format.

Web Monitor: The user interface of MM ShutdownAgent used to monitor and configure the software.



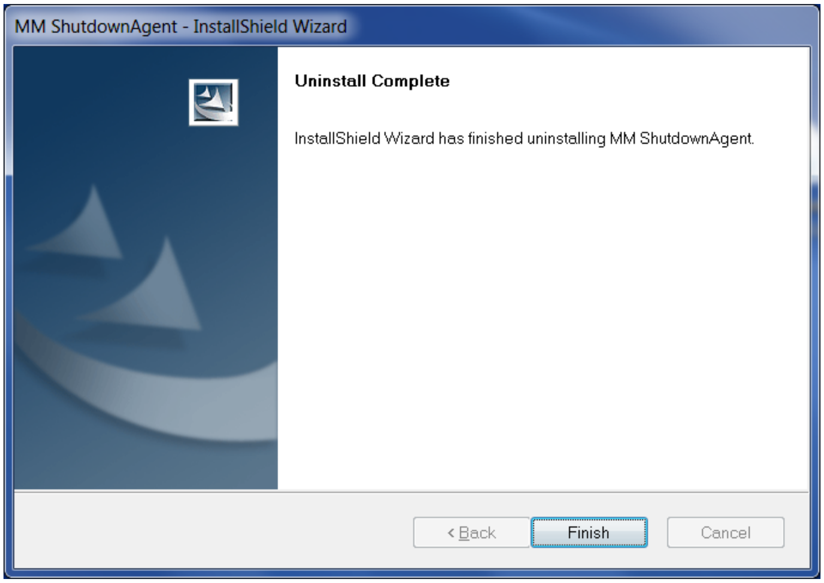
2.1.2 Uninstall Process

1. Select the Uninstall from the MM ShutdownAgent program folder to start the uninstall process. Or you can start the MM ShutdownAgent uninstall process from the Add/Remove Program in the Control Panel.
2. Press the OK button to confirm removing all of the application or the Cancel button to cancel the uninstall process.


MM ShutdownAgent - InstallShield Wizard

Do you want to completely remove the selected application and all of its features?

3. Press the Finish button to complete the uninstall process.


MM ShutdownAgent - InstallShield Wizard

Uninstall Complete

InstallShield Wizard has finished uninstalling MM ShutdownAgent.

2.2 For Linux System

2.2.1 Installation Process

1. Login to the Linux system and change to the root account:
   su root
2. Copy the MM-Shutdownagent-linux.tar.gz to the /tmp directory:
   cp MM-Shutdownagent -linux.tar.gz /tmp
3. Change your working directory to /tmp:
   cd /tmp
4. uncompress the MM-Shutdownagent -linux.tar.gz:
   gunzip MM-Shutdownagent -linux.tar.gz

5. extract the MM-Shutdownagent -linux.tar:
   tar xvf MM-Shutdownagent -linux.tar
6. Run the install script:
   ./install

```
+-----------------------------------------------+
|  MM ShutdownAgent 0.0.1 for Linux     |
|  Copyright (c) 2012, Minuteman UPS.  |
|  All Rights Reserved.                         |
+-----------------------------------------------+

Do you want to install the MM ShutdownAgent? [y|n]
```

7. Press ‘y’ to proceed with the installation process:

```
+-----------------------------------------------+
|  MM ShutdownAgent 0.0.1 for Linux     |
|  Copyright (c) 2012 Minuteman UPS.  |
|  All Rights Reserved.                         |
+-----------------------------------------------+

The destination directory is /usr/local/upsagent.

Copying files ..............
Install service link.

shutdownagent             0:off  1:off  2:off  3:on   4:off  5:on   6:off

Starting MM ShutdownAgent(upsagentd) ... done

Do you want to configure the MM ShutdownAgent right now? [y|n]
```

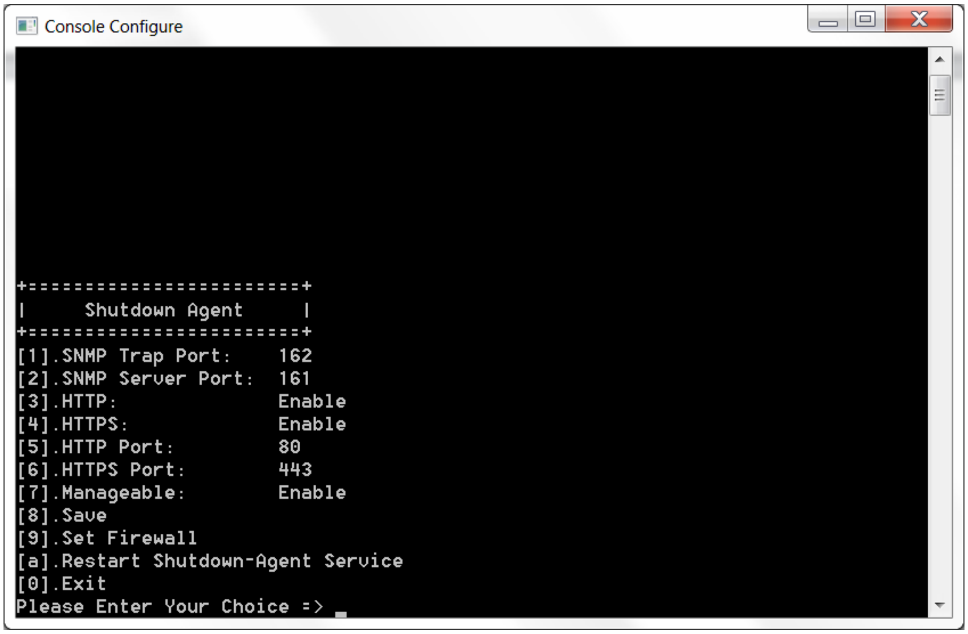
8. Now the MM ShutdownAgent has been installed in the following directory /usr/local/upsagent/ and the service program will automatically start up.
   Press ‘y’ to launch the /usr/local/upsagent/configure program to configure the basic parameters for the MM ShutdownAgent or press ‘n’ to finish the install process.
   See Chapter 3 for more information if you want to configure the basic parameters.

2.2.2 Uninstall Process

1. Login to the Linux system and change to the root account:
   su root
2. Change your working directory to /usr/local/upsagent:
   cd /usr/local/upsagent
3. Run the uninstall script to remove the MM ShutdownAgent:
   ./uninstall
4. Press ‘y’ to start the uninstall process.

3. Console Configuration

The configuration program is design to do the basic configuration for the MM ShutdownAgent in the shell mode. The software can be launched at the end of the installation process or you can go to the installed directory to launch it manually.
For Windows it is located in “C:\Program Files\MM Shutdown Agent\Agent-Config.exe”
For Linux it is located in “/usr/local/upsagent/configure”



```
+========================+
|     Shutdown Agent     |
+========================+
[1].SNMP Trap Port:    162
[2].SNMP Server Port:  161
[3].HTTP:              Enable
[4].HTTPS:             Enable
[5].HTTP Port:         80
[6].HTTPS Port:        443
[7].Manageable:        Enable
[8].Save
[9].Set Firewall
[a].Restart Shutdown-Agent Service
[0].Exit
Please Enter Your Choice => _
```

3.1 Console Menu

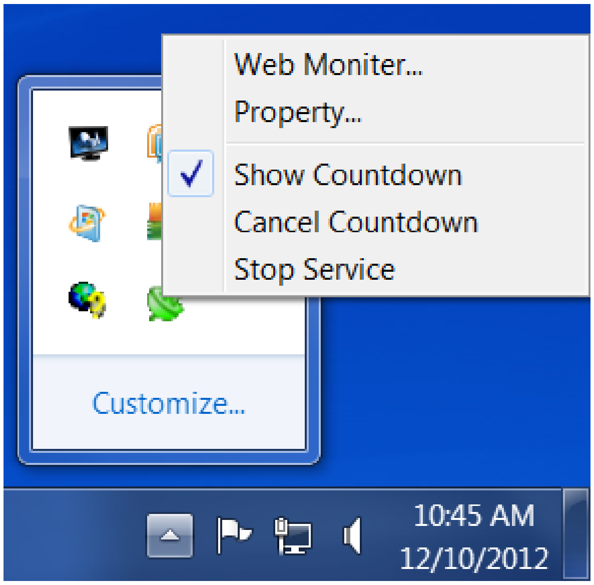
No.	**Function**	**Description**	**Default**
1.	SNMP Trap Port	The UDP port to listen for the SNMP trap	162
2.	SNMP Server Port	The UDP port for replying to get/set commands	161
3.	HTTP	Enable or disable the HTTP protocol	Enable
4.	HTTPS	Enable or disable the HTTPS protocol	Enable
5.	HTTP Port	The TCP port for HTTP	80
6.	HTTPS Port	The TCP port for HTTPS	443
7.	Manageable	Allow a management software to manage the ShutdownAgent	Enable
8.	Save	Save the configured parameters to agent.ini	
9.	Set Firewall	Insert or remove the firewall rule for the ShutdownAgent. This option is provided for quickly testing the network communication. The firewall settings may be recovered after the OS reboots.	
a.	Restart Shutdown-Agent Service	Restart the service program to apply the changes	
0.	Exit	Exit the configuration program	

4. Operation in Windows

After the installation, the ShutdownAgent places an icon in the desktop toolbar to indicate the status of the monitored UPS.

Icon	Description
🟩	Normal
🟥	Service stop
🟦	UPS on battery mode
🟥	UPS battery low
🟪	UPS on bypass mode

To show the pop-up menu, move the cursor over the ShutdownAgent icon and right click to open the menu.



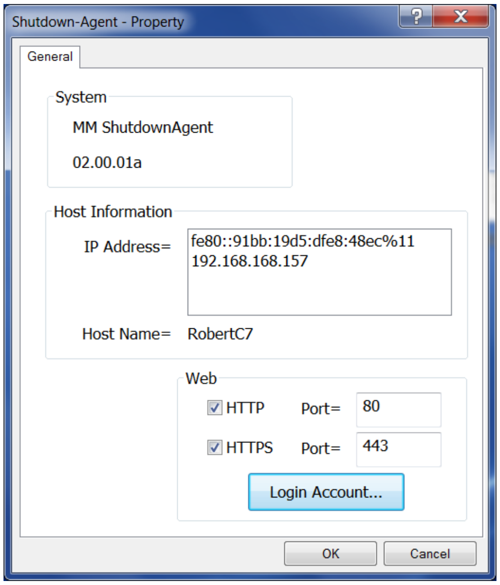
4.1 Web Monitor

The ShutdownAgent uses a web interface to monitor and configure the software. Select the **Web Monitor** menu to launch the default web browser. If your login account in Windows belongs to the local Administrator group then the ShutdownAgent will login to its web browser automatically as the administrator. If you connect a web browser from a remote PC then you have to key in the User Name and Password. The default User Name is **admin** and the default Password is **password**.

For more detail information about the web operation, refer to Chapter 5.

4.2 Property

The **Property** menu provides another way to configure the basic parameters of the ShutdownAgent. The General tab displays the software version number, the IP address of the PC that the software is installed on, the host name and the ports.



MM ShutdownAgent
02.00.01a
IP Address= fe80::91bb:19d5:dfe8:48ec%11
192.168.168.157
Host Name= RobertC7
☑ HTTP Port= 80
☑ HTTPS Port= 443

HTTP:

To enable / disable the HTTP protocol, assign a different number for the Port to change the HTTP connection. The default port is 80. If you change the HTTP port from 80 then you have to key in the URL as the follows: http://192.168.1.100:8001
192.168.1.100 is the IP address of the PC that the ShutdownAgent is installed on and 8001 is the port number you assigned.
NOTE: Check the Windows firewall setting if the HTTP connection is refused.

HTTPS:

To enable / disable the HTTPS protocol, assign a different number for the Port to change the HTTPS connection. The default port is 443. If you have change the HTTPS port from 443 then you have to key in the URL as the follows: https://192.168.1.100:4430
192.168.1.100 is the IP address of the PC that the ShutdownAgent is installed on and 4430 is the port number you assigned.
NOTE: Check the Windows firewall setting if the HTTPS connection is refused.

Login Account:

The ShutdownAgent implements 3 levels of authentication for the web login as follows:

Administrator:

Has the sole right to modify the ShutdownAgent settings.

Device Manager:

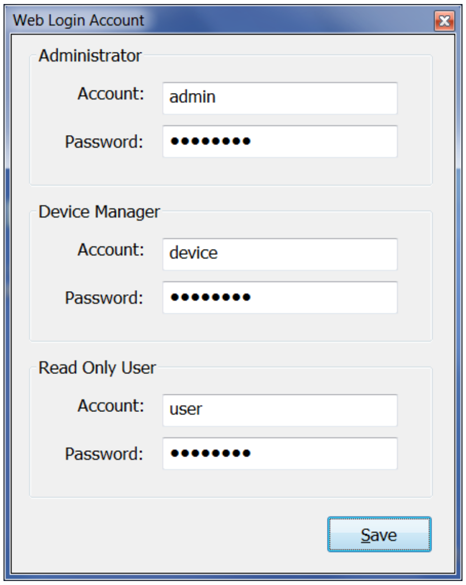
Is not permitted to change the system settings but has the ability to configure the device settings.

Read Only User:

The user is only permitted to observe the connected devices.

The following is the default account and password list. Note they are case-sensitive.

	Account	**Password**
Administrator	admin	password
Device Manager	device	password
Read Only User	user	password



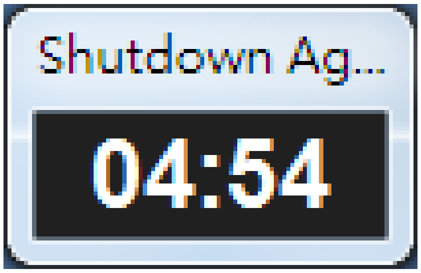
Administrator
Account: admin
Password: ••••••••

Device Manager
Account: device
Password: ••••••••

Read Only User
Account: user
Password: ••••••••

4.3 Show Countdown

The Show Countdown will display the countdown window when the ShutdownAgent starts the countdown for the OS shutdown.



4.4 Cancel Countdown

Select the Cancel Countdown during the countdown to stop the shutdown process. To resume the shutdown process, de-select the Cancel Countdown.

NOTE: On a new shutdown event the countdown will be displayed.

4.5 Stop Service

Select the Stop Service to stop the ShutdownAgent service module. To start the services again de-select the Stop Service item.

5. Web Interface

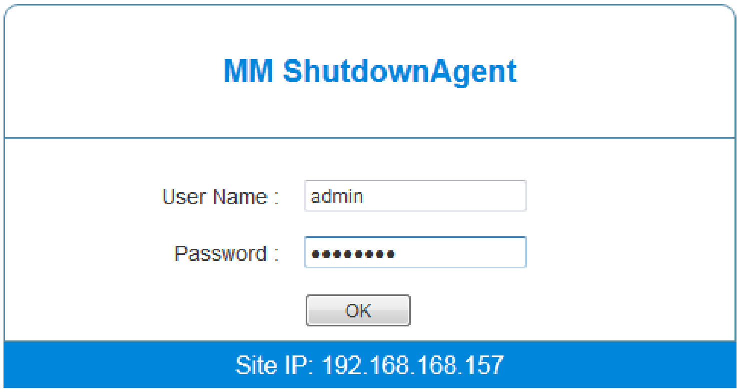
5.1 Run a Web Browser

To connect to a web browser from the same PC which ShutdownAgent is installed on, select the **Web Monitor** from the toolbar menu, the ShutdownAgent will open your default web browser and if your Windows account belongs to the local Administrator group then the ShutdownAgent will automatically login as the administrator.

The ShutdownAgent allows a maximum of 16 users to login at the same time.

You can also connect with a web browser from a remote PC, as follows:
Make sure that you have a **TCP/IP** network installed.
Start your Web Browser. Enter **http: //host_name** or **http: //ip_address** in the address bar for the plain text web transmission or **https: //host_name** or **https: //ip_address** for the encrypted web transmission. If you have changed the port number for the HTTP or the HTTPS connection, then enter **http: //host_name:port_number** or **http: //ip_address:port_number** in the address bar for the plain text web transmission or **https: //host_name:port_number** or **https: //ip_address:port_number** for the encrypted web transmission.

The ShutdownAgent will then ask for your user name and password. After keying in the correct **User Name** and **Password**, the **ShutdownAgent Home Page** will open.



MM ShutdownAgent

User Name : admin

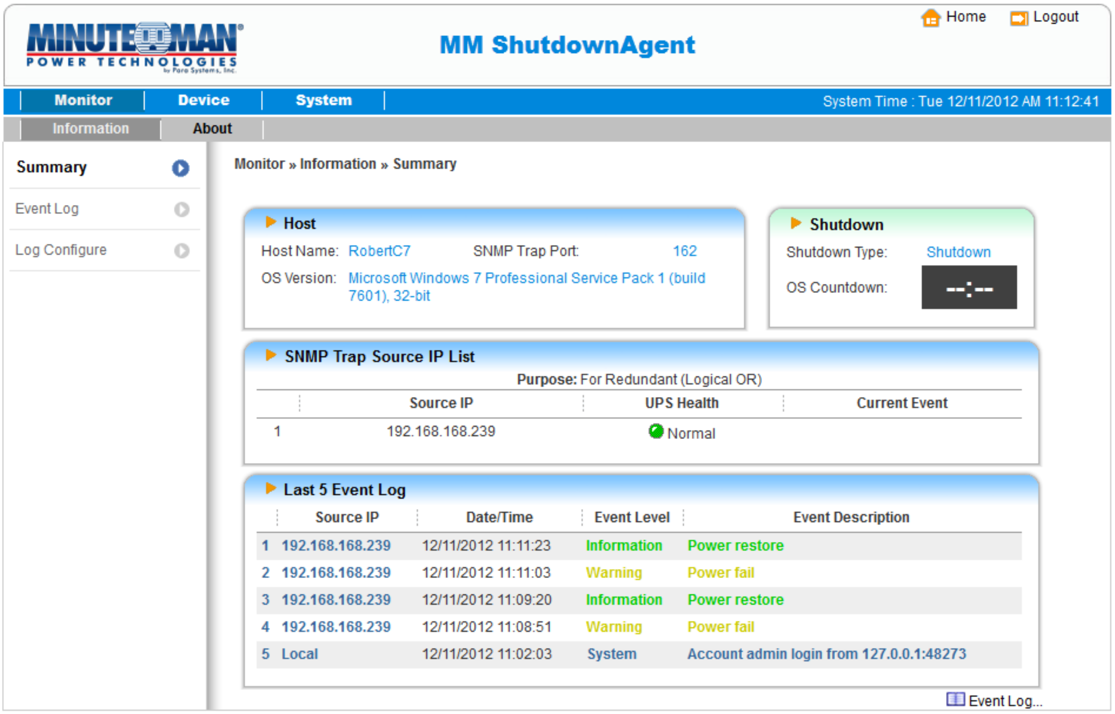
Password : ••••••••

Site IP: 192.168.168.157

NOTE: The ShutdownAgent will automatically logout the user if there is no data transmission for 30 minutes.

5.2 Monitor >> Information >> Summary

This page has information about the host, the shutdown status, the SNMP Trap source IP status and the last 5 events.



System Time : Tue 12/11/2012 AM 11:12:41

Monitor » Information » Summary

Host

Host Name: RobertC7

SNMP Trap Port: 162

OS Version: Microsoft Windows 7 Professional Service Pack 1 (build 7601), 32-bit

Shutdown

Shutdown Type: Shutdown

OS Countdown: --:--

SNMP Trap Source IP List

Purpose: For Redundant (Logical OR)

	Source IP	UPS Health	Current Event
1	192.168.168.239	Normal	

Last 5 Event Log

	Source IP	Date/Time	Event Level	Event Description
1	192.168.168.239	12/11/2012 11:11:23	Information	Power restore
2	192.168.168.239	12/11/2012 11:11:03	Warning	Power fail
3	192.168.168.239	12/11/2012 11:09:20	Information	Power restore
4	192.168.168.239	12/11/2012 11:08:51	Warning	Power fail
5	Local	12/11/2012 11:02:03	System	Account admin login from 127.0.0.1:48273

Host:

List the host name, the UDP port for SNMP traps and the operating system.

Shutdown:

Displays the shutdown type (Shutdown, Power Off, Hibernate) and the countdown time to shutdown the OS (when activated). The time is displayed in seconds.

SNMP Trap Source IP List:

The ShutdownAgent is capable of receiving SNMP traps from multiple source hosts then list the event as logical OR for redundant application or logical AND for parallel application.

Last 5 Event Log:

Shows the last 5 events logged. To see the entire list of the Events logged click on the Event Log at the bottom right corner of this page or click on the Event Log page.

5.3 Monitor >> Information >> Event Log

This web page lists all the events that have been detected by the software. The existing logs are overwritten when the maximum number of entries (rows) has been reached. And the maximum number of events is 10,000. You can download the event log in a .csv file format.

Log Page Buttons:

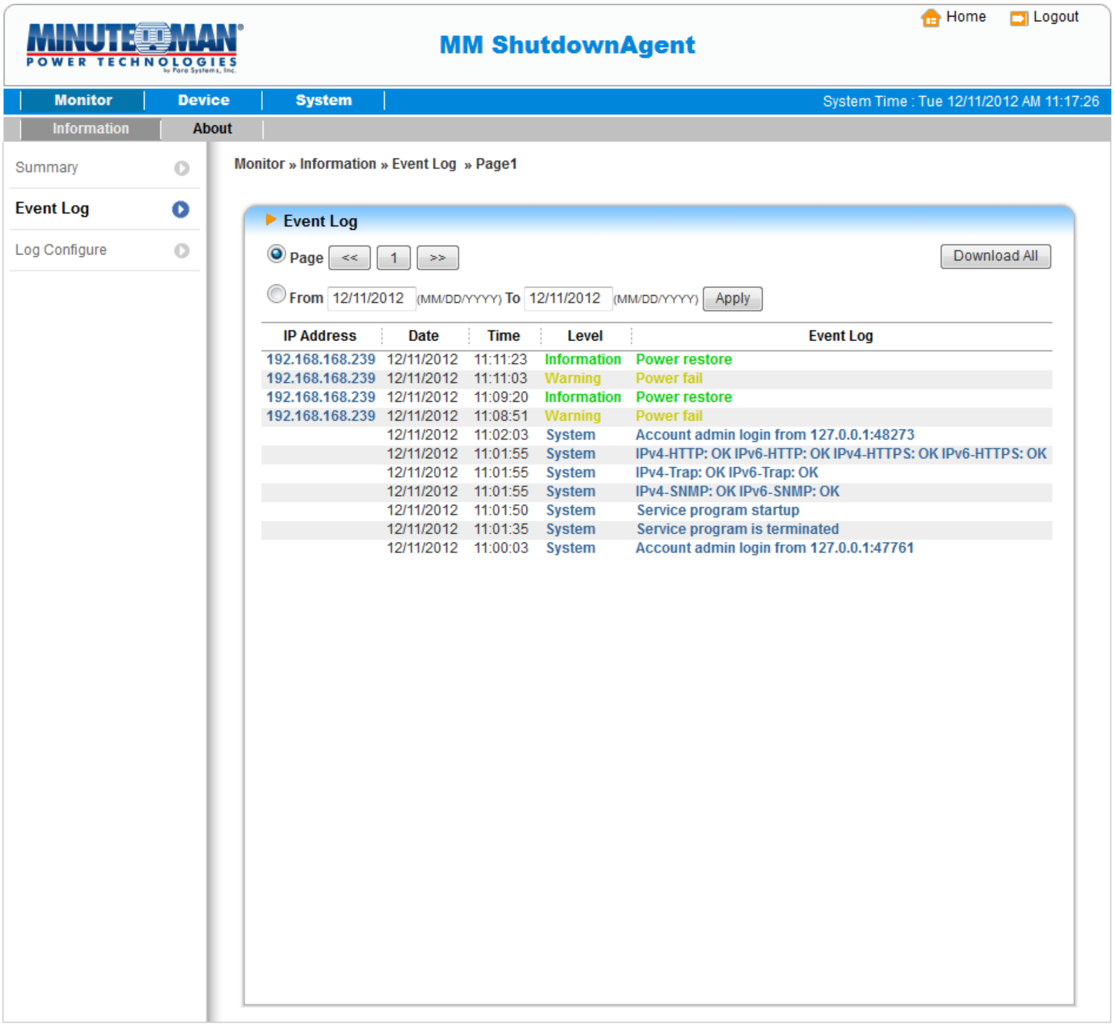
Press the “**<<**” button to go to the newest page and the “**>>**” button to go to the oldest page. Click on the page number buttons to display the event log by page.

From and To Dates:

You can filter the event log by a range of dates. Enter the dates and then press the Apply button.

Download All:

Press the **Download All** button to export the entire event log in a .csv file format.



System Time : Tue 12/11/2012 AM 11:17:26

Monitor » Information » Event Log » Page1

● Page ○ From 12/11/2012 (MM/DD/YYYY) To 12/11/2012 (MM/DD/YYYY)

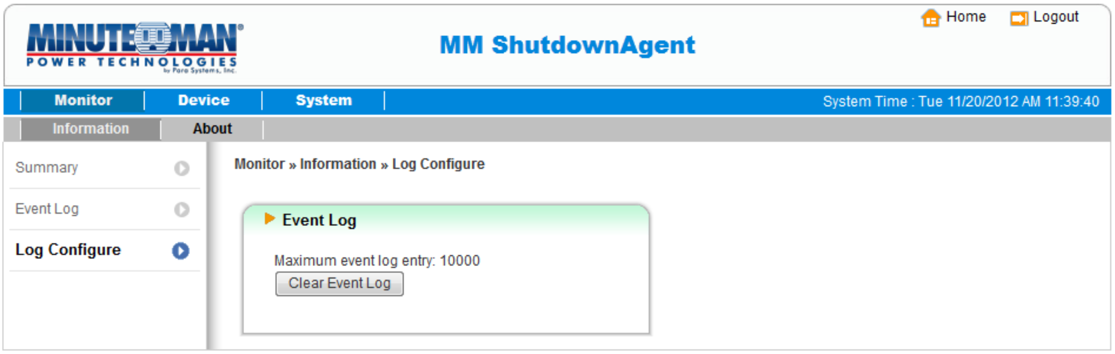
IP Address	Date	Time	Level	Event Log
192.168.168.239	12/11/2012	11:11:23	Information	Power restore
192.168.168.239	12/11/2012	11:11:03	Warning	Power fail
192.168.168.239	12/11/2012	11:09:20	Information	Power restore
192.168.168.239	12/11/2012	11:08:51	Warning	Power fail
	12/11/2012	11:02:03	System	Account admin login from 127.0.0.1:48273
	12/11/2012	11:01:55	System	IPv4-HTTP: OK IPv6-HTTP: OK IPv4-HTTPS: OK IPv6-HTTPS: OK
	12/11/2012	11:01:55	System	IPv4-Trap: OK IPv6-Trap: OK
	12/11/2012	11:01:55	System	IPv4-SNMP: OK IPv6-SNMP: OK
	12/11/2012	11:01:50	System	Service program startup
	12/11/2012	11:01:35	System	Service program is terminated
	12/11/2012	11:00:03	System	Account admin login from 127.0.0.1:47761

5.4 Monitor >> Information >> Log Configure

This page allows you to clear the event log.

Clear Event Log:

Click on this button to clear the event log.



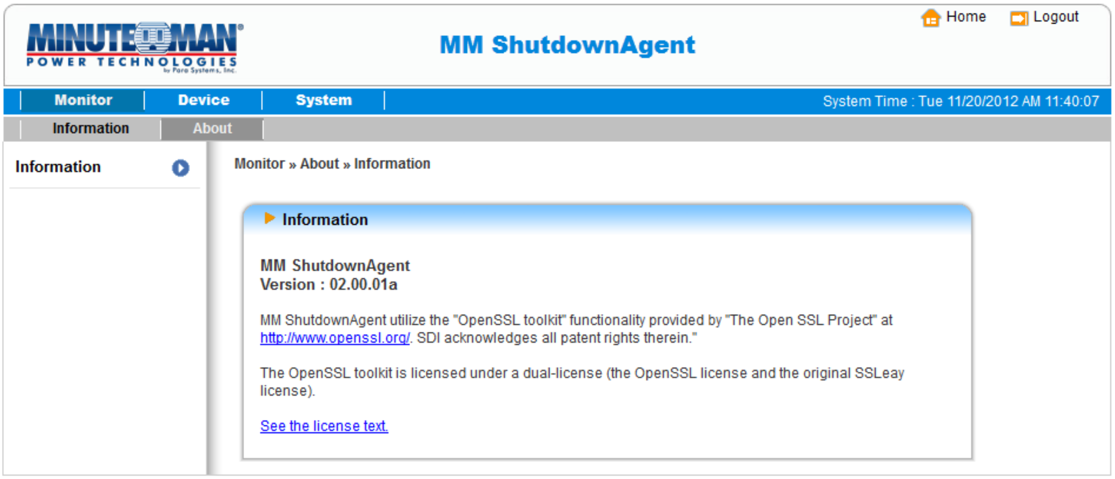
System Time : Tue 11/20/2012 AM 11:39:40

Monitor » Information » Log Configure

Maximum event log entry: 10000

5.5 Monitor >> About >> Information

This page displays the version number of the software and important information about the SSL toolkit used by this software.



System Time : Tue 11/20/2012 AM 11:40:07

Monitor » About » Information

MM ShutdownAgent
Version : 02.00.01a

MM ShutdownAgent utilize the "OpenSSL toolkit" functionality provided by "The Open SSL Project" at http://www.openssl.org/. SDI acknowledges all patent rights therein."

The OpenSSL toolkit is licensed under a dual-license (the OpenSSL license and the original SSLeay license).

See the license text.

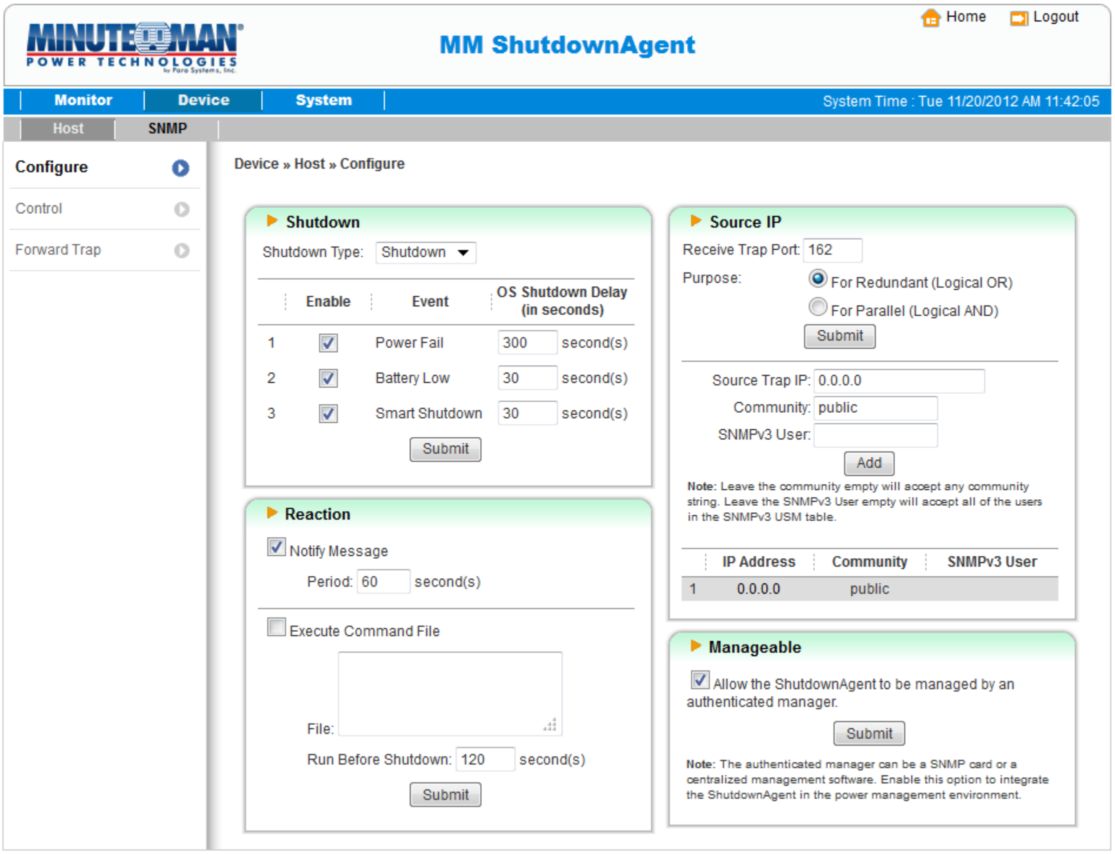
5.6 Device >> Host >> Configure

This page is used to configure the following functions: Shutdown, Reaction, Source IP and Manageable.

Shutdown:

Select the appropriate **Shutdown Type** to shutdown the operating system. There are three selections for the Shutdown type: **Shutdown**, **Power Off** and **Hibernate**. The default is Shutdown.

Set the Shutdown Delay time for the Enabled Power Event. If the power event recovers during the countdown then the Shutdown action will be terminated.



System Time : Tue 11/20/2012 AM 11:42:05

Device » Host » Configure

Shutdown

Shutdown Type: Shutdown

	Enable	Event	OS Shutdown Delay (in seconds)
1	☑	Power Fail	300 second(s)
2	☑	Battery Low	30 second(s)
3	☑	Smart Shutdown	30 second(s)

Reaction

☑ Notify Message

Period: 60 second(s)

☐ Execute Command File

File:

Run Before Shutdown: 120 second(s)

Source IP

Receive Trap Port: 162

Purpose: ● For Redundant (Logical OR)

○ For Parallel (Logical AND)

Source Trap IP: 0.0.0.0

Community: public

SNMPv3 User:

Note: Leave the community empty will accept any community string. Leave the SNMPv3 User empty will accept all of the users in the SNMPv3 USM table.

	IP Address	Community	SNMPv3 User
1	0.0.0.0	public	

Manageable

☑ Allow the ShutdownAgent to be managed by an authenticated manager.

Note: The authenticated manager can be a SNMP card or a centralized management software. Enable this option to integrate the ShutdownAgent in the power management environment.

Reaction:

Enable the **Notify Message** to receive pop-up messages once the ShutdownAgent receives an SNMP trap. Assign the period time to report the message periodically, setting the time period to 0-seconds will show the message only once.

Enable the **Execute Command File** to run an assigned external file before shutting down. Set a time to the **Run Before Shutdown** to inform ShutdownAgent when to launch the assigned executable file.

Source IP:

Assign the **Receive Trap Port** to open a specific UDP port for receiving SNMP traps. Then select the Redundant (Logical OR) or Parallel (Logical AND) for the application purpose.

Redundant (Logical OR): Summarizes the received power event by logical OR for all of the source IP addresses to determine whether the power event occurred or not. If the power event occurred in one of the source IP addresses then the power event is tenable and the ShutdownAgent starts to countdown accordingly. Only when the power event recovers from all of the source IP addresses will the ShutdownAgent stop and cancel the shutdown process.

Parallel (Logical AND): Summarizes the received power event by logical AND for all of the source IP addresses to determine whether the power event occurred or not. If the power event occurred in all of the source IP addresses then the power event is tenable and the ShutdownAgent starts to countdown accordingly. Once the power event recovers from one of the source IP addresses the ShutdownAgent will stop and cancel the shutdown process.

Source IP Address: Assign the source IP address. The ShutdownAgent will only parse the SNMP trap when the packet is received from the assigned IP addresses.

Community: If there is an assigned community string value then only the received trap with the same community string will be accepted. If there is no community string assigned then ShutdownAgent will accept any of the received community strings.

SNMPv3 User: This field is used for the SNMPv3 packets. If there is an assigned SNMPv3 User then only the received trap with the same user defined in the SNMPv3 USM table will be accepted. If there is not a SNMPv3 User assigned then ShutdownAgent will not accept the users which are assigned in the SNMPv3 USM table.

Manageable:

Select the **Allow the ShutdownAgent to be managed by an authenticated manager** option to let the ShutdownAgent reply to the query from any authenticated manager. The authenticated manager can be a SNMP card or a centralized management software. After collecting the ShutdownAgent information, the authenticated manager can provide a comprehensive list of all of the ShutdownAgents.

The authenticated manager communicates with the ShutdownAgent through SNMPv3 with the first default account in the SNMPv3 USM list. If this option is enabled then the manager’s account changes to “Read/Write”, otherwise the permission is “Disable”. The default setting for the **Allow the ShutdownAgent to be managed by an authenticated manager** is enabled.

5.7 Device >> Host >> Control

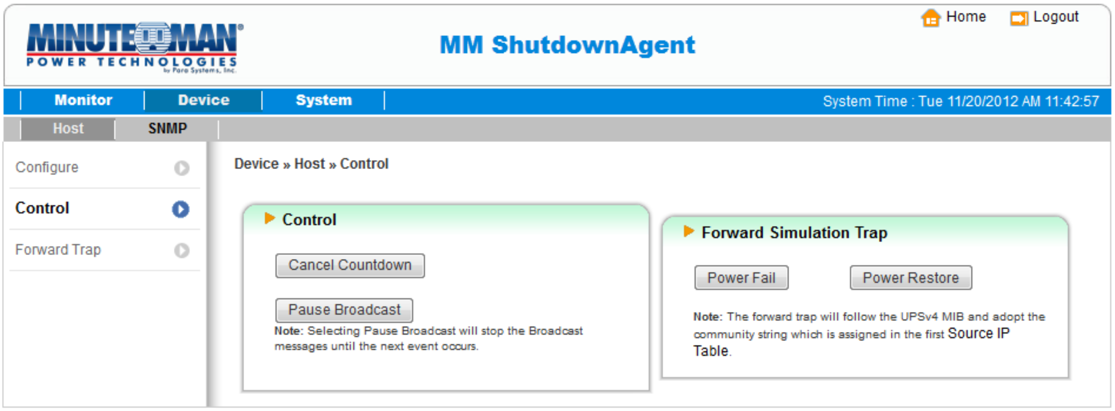
Control:

Press the Cancel Countdown button during the countdown process to stop the shutdown. Press the button again to resume the shutdown process.

Forward Simulation Trap:

Press the Power Fail button to send the simulated power fail SNMP trap to the assigned forward target IP addresses.

Press the Power Restore button to send the simulated power restore SNMP trap to the assigned forward target IP addresses.



System Time : Tue 11/20/2012 AM 11:42:57

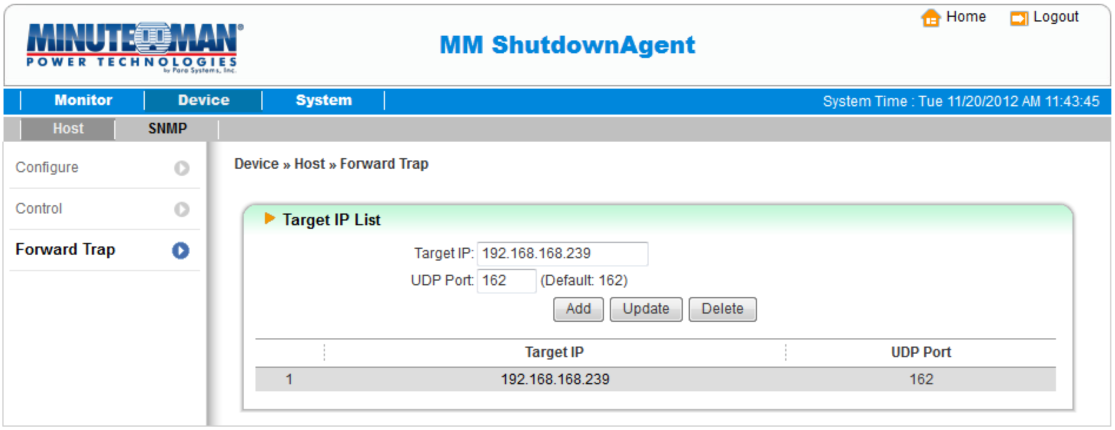
Device » Host » Control

Note: Selecting Pause Broadcast will stop the Broadcast messages until the next event occurs.

Note: The forward trap will follow the UPSv4 MIB and adopt the community string which is assigned in the first Source IP Table.

5.8 Device >> Host >> Forward Trap

The Forward Trap is used to forward the received SNMP traps to the targeted IP addresses to perform the shutdown.



System Time : Tue 11/20/2012 AM 11:43:45

Device » Host » Forward Trap

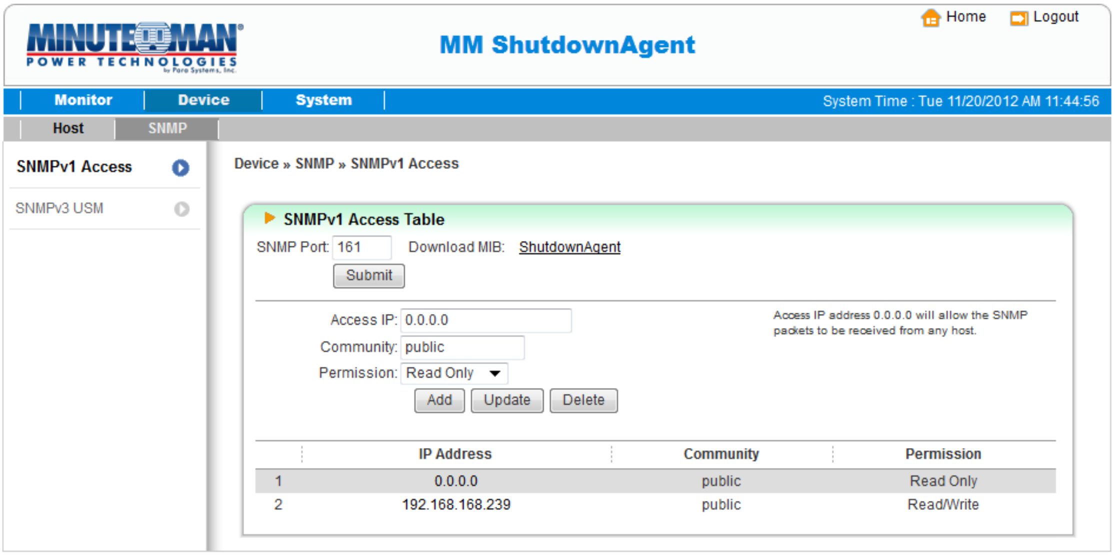
Target IP: 192.168.168.239

UDP Port: 162 (Default: 162)

	Target IP	UDP Port
1	192.168.168.239	162

5.9 Device >> SNMP >> SNMP Access

The ShutdownAgent supports SNMP protocol and SNMP NMS (Network Management System), which are commonly used to monitor network devices for conditions that call for administrative attention. To prevent unauthorized access, you can specify the NMS IP addresses, their community strings and access levels. The maximum number of IP entries is 255.



System Time : Tue 11/20/2012 AM 11:44:56

Device » SNMP » SNMPv1 Access

SNMPv1 Access Table

SNMP Port: 161 Download MIB: ShutdownAgent

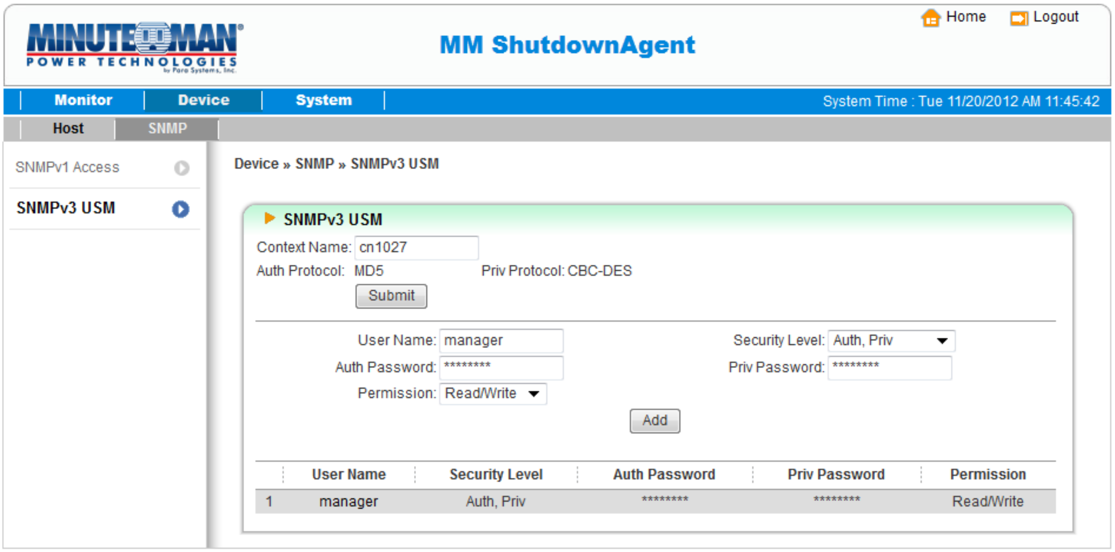
Access IP: 0.0.0.0
Community: public
Permission: Read Only

Access IP address 0.0.0.0 will allow the SNMP packets to be received from any host.

	IP Address	Community	Permission
1	0.0.0.0	public	Read Only
2	192.168.168.239	public	Read/Write

5.10 Device >> SNMP >> SNMPv3 USM

SNMPv3 offers features such as the encryption of packets and authentication to improve security. The SNMPv3 USM (User Session Management) allows you to assign 32 User Names. You can also define their respective Security Levels, Auth Passwords, Priv Passwords and Permission. The first account cannot be deleted, to disable it go to the Device >> Host >> Configure web page then uncheck the manageable option.



System Time : Tue 11/20/2012 AM 11:45:42

Device » SNMP » SNMPv3 USM

SNMPv3 USM

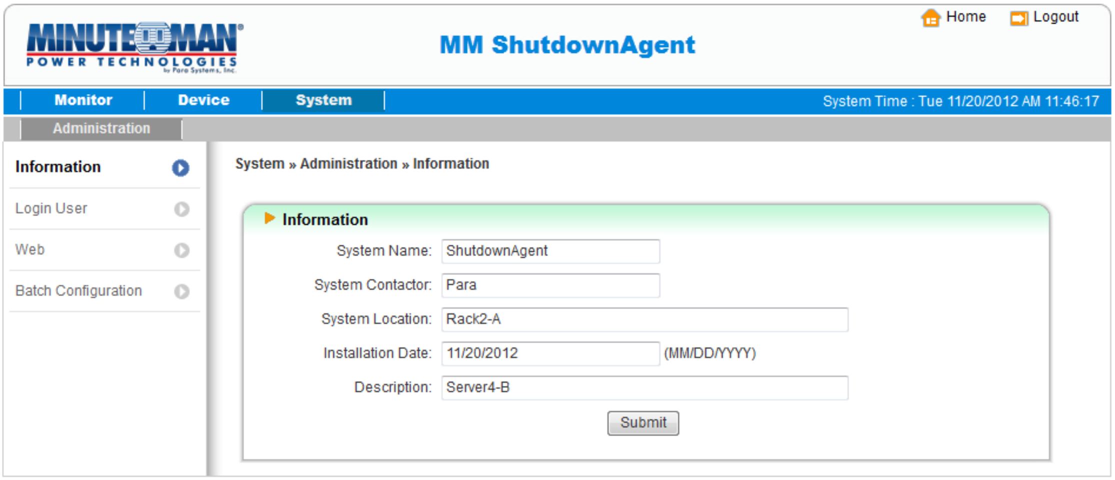
Context Name: cn1027
Auth Protocol: MD5 Priv Protocol: CBC-DES

User Name: manager
Security Level: Auth, Priv
Auth Password: ********
Priv Password: ********
Permission: Read/Write

	User Name	Security Level	Auth Password	Priv Password	Permission
1	manager	Auth, Priv	********	********	Read/Write

5.11 System >> Administration >> Information

The system information can be configured here.



System Time : Tue 11/20/2012 AM 11:46:17

System » Administration » Information

Information

System Name: ShutdownAgent

System Contactor: Para

System Location: Rack2-A

Installation Date: 11/20/2012 (MM/DD/YYYY)

Description: Server4-B

5.12 System >> Administration >> Login User

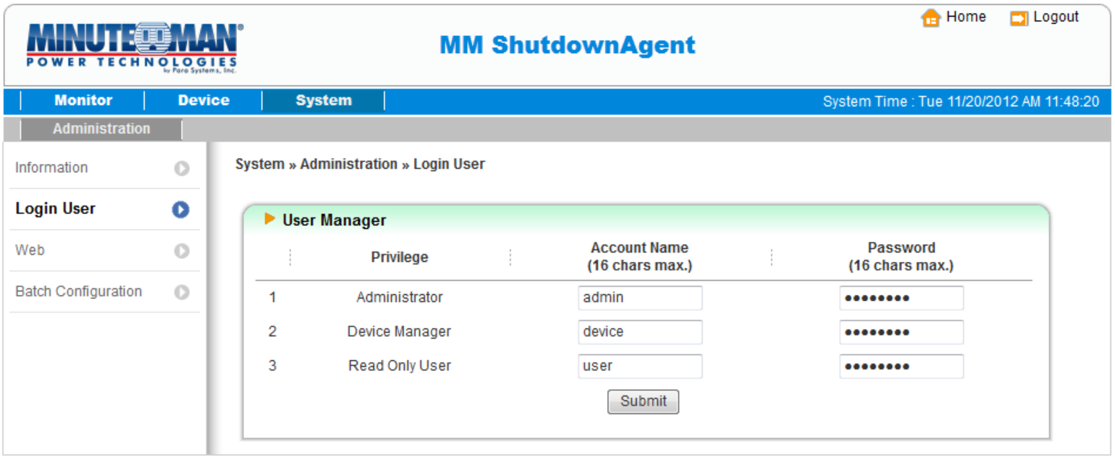
The login authentication for the web interface can be managed by assigning the three different levels for the users' account and password.

The access permission for the account types are listed as follows:

Administrator: Permitted to modify all settings.

Device Manager: Permitted to modify device-related settings.

Read Only User: Permitted to Read Only the ShutdownAgent status.



System Time : Tue 11/20/2012 AM 11:48:20

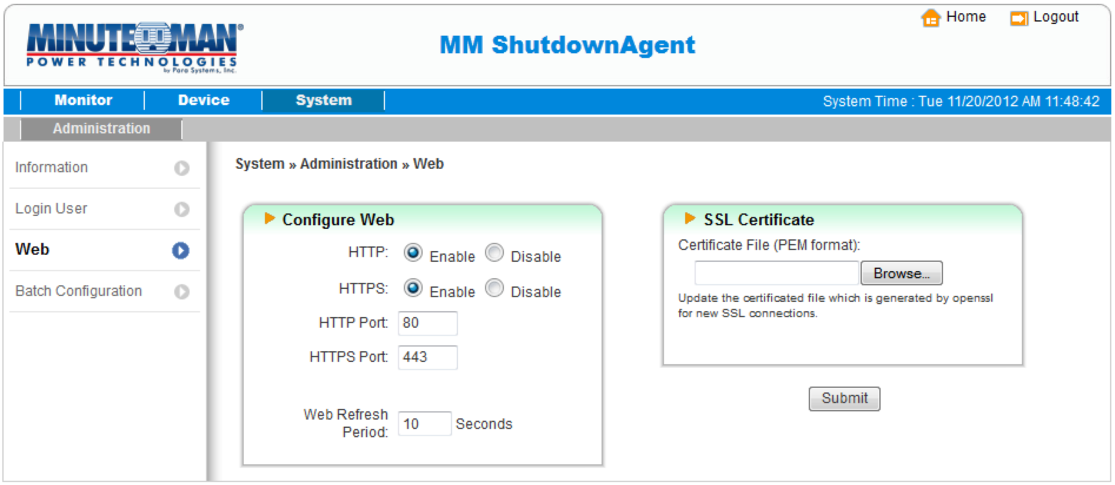
System » Administration » Login User

User Manager

	Privilege	Account Name (16 chars max.)	Password (16 chars max.)
1	Administrator	admin	••••••••
2	Device Manager	device	••••••••
3	Read Only User	user	••••••••

5.13 System >> Administration >> Web

This menu lets the administrator enable or disable the HTTP/HTTPS communication protocols available in the ShutdownAgent.



System Time : Tue 11/20/2012 AM 11:48:42

System » Administration » Web

Configure Web

HTTP: ● Enable ○ Disable

HTTPS: ● Enable ○ Disable

HTTP Port: 80

HTTPS Port: 443

Web Refresh Period: 10 Seconds

SSL Certificate

Certificate File (PEM format):

Update the certificated file which is generated by openssl for new SSL connections.

HTTP:

Enabling or disabling the HTTP connection with the ShutdownAgent.

HTTPS:

Enabling or disabling the HTTPS connection with the ShutdownAgent.

HTTP Port:

The user may configure HTTP protocol to use a port number other than standard HTTP port (80).

HTTPS Port:

The user may configure HTTPS protocol to use a port number other than standard HTTPS port (443).

Web Refresh Period:

The time interval for refreshing the web page can be configured. The range is 1~9999 seconds.

SSL Certificate:

To ensure the security between the ShutdownAgent and the connecting workstation, the SSL certificate can be used to encrypt and secure the integrity of the transmitted data.

Certificate File: This allows you to replace your own SSL certificate file. The ShutdownAgent supports PEM format which is generated by OpenSSL. Click **Choose File** to upload the certificate file.

5.14 System >> Administration >> Batch Configuration

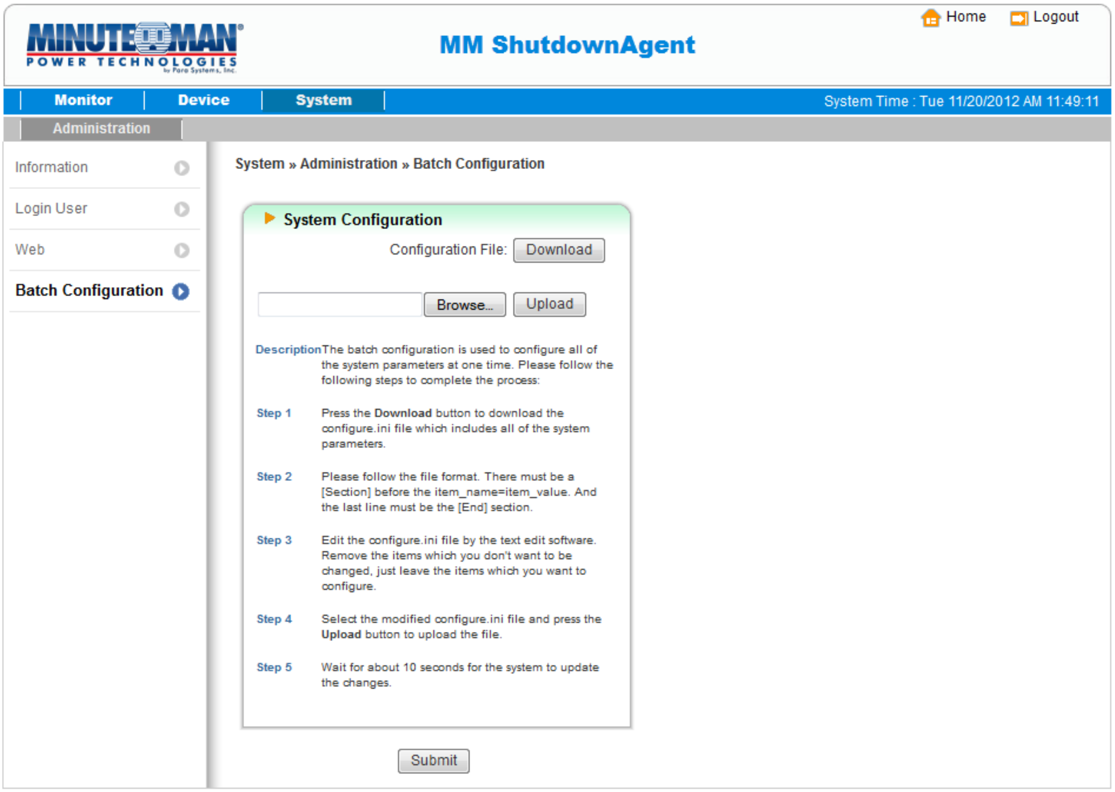
The ShutdownAgent provides batch configuration to allow quick and effortless setup on multiple ShutdownAgent hosts. You can duplicate the settings by downloading the configuration file from the ShutdownAgent that you have successfully configured, and upload the configuration files to multiple ShutdownAgents. Simply follow the step by step procedure.

Download:

Download the agent.ini file to store or edit the configuration file.

Upload:

Upload the configuration file to multiple ShutdownAgents.



Description The batch configuration is used to configure all of the system parameters at one time. Please follow the following steps to complete the process:

Step 1 Press the **Download** button to download the configure.ini file which includes all of the system parameters.

Step 2 Please follow the file format. There must be a [Section] before the item_name=item_value. And the last line must be the [End] section.

Step 3 Edit the configure.ini file by the text edit software. Remove the items which you don't want to be changed, just leave the items which you want to configure.

Step 4 Select the modified configure.ini file and press the **Upload** button to upload the file.

Step 5 Wait for about 10 seconds for the system to update the changes.

6. 2008 Server Core Setup for the ShutdownAgent

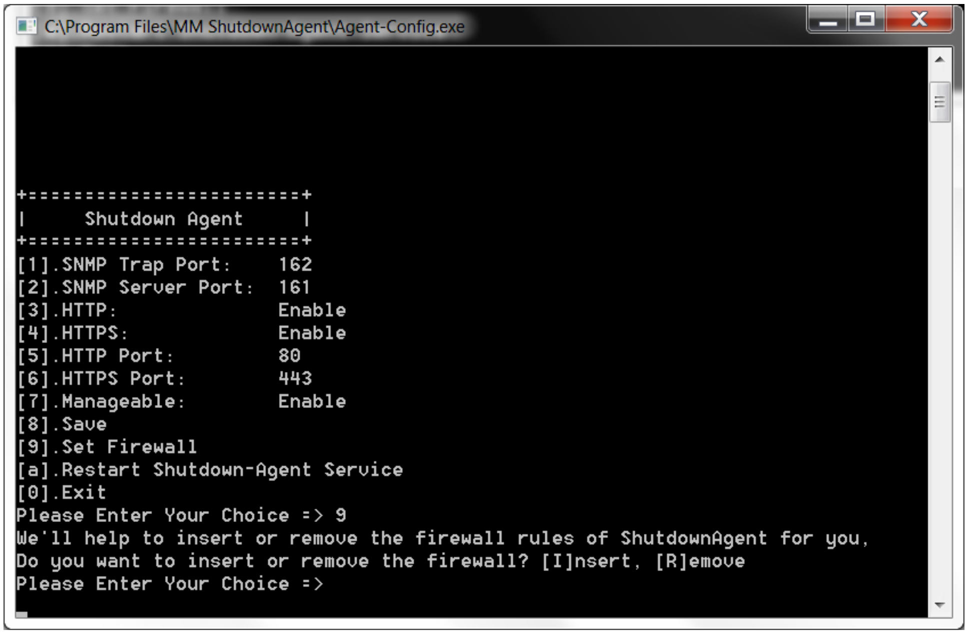
When installing the ShutdownAgent for the 2008 server core, it requires the following commands to transfer the file and add rules for firewall.

1. Disable the firewall:
   ```
   netsh advfirewall set allprofiles state off
   ```
2. Enable the firewall:
   ```
   netsh advfirewall set allprofiles state on
   ```
3. Add a remotely shared directory:
   ```
   net use e: \\<ip address>\e
   ```
4. Open the SNMP Trap UDP 162
   ```
   netsh advfirewall firewall add rule name="SNMPTrap" protocol=UDP dir=in localport=162 action = allow
   ```
5. Open the SNMP Server UDP 161
   ```
   netsh advfirewall firewall add rule name="SNMPServer" protocol=UDP dir=in localport=161 action = allow
   ```
6. Open the HTTP TCP 80
   ```
   netsh advfirewall firewall add rule name="HTTP" protocol=TCP dir=in localport=80 action = allow
   ```
7. Open the HTTPS TCP 443
   ```
   netsh advfirewall firewall add rule name="HTTPS" protocol=TCP dir=in localport=443 action = allow
   ```

First, put the Shutdown-Agent-2012-Setup(x64).exe setup file in the 2008 server directory. If there is no CD-ROM you can set the “Disable firewall” command, “Add a remotely shared directory” command then copy the file from your PC to the 2008 server. Do not forget to set the “Enable firewall” command when completed.

Second, follow Chapter 2 to install the ShutdownAgent in the 2008 server. The last step is to use the open HTTP/HTTPS, SNMP Trap/Server port commands to open the necessary ports. You can easily run the Agent-Config.exe to configure the basic networking parameters for the web and SNMP network protocols after the installation.

Select [9] to configure the firewall for the ShutdownAgent.



```
+========================+
|     Shutdown Agent     |
+========================+
[1].SNMP Trap Port:    162
[2].SNMP Server Port:  161
[3].HTTP:              Enable
[4].HTTPS:             Enable
[5].HTTP Port:         80
[6].HTTPS Port:        443
[7].Manageable:        Enable
[8].Save
[9].Set Firewall
[a].Restart Shutdown-Agent Service
[0].Exit
Please Enter Your Choice => 9
We'll help to insert or remove the firewall rules of ShutdownAgent for you,
Do you want to insert or remove the firewall? [I]nsert, [R]emove
Please Enter Your Choice =>
```

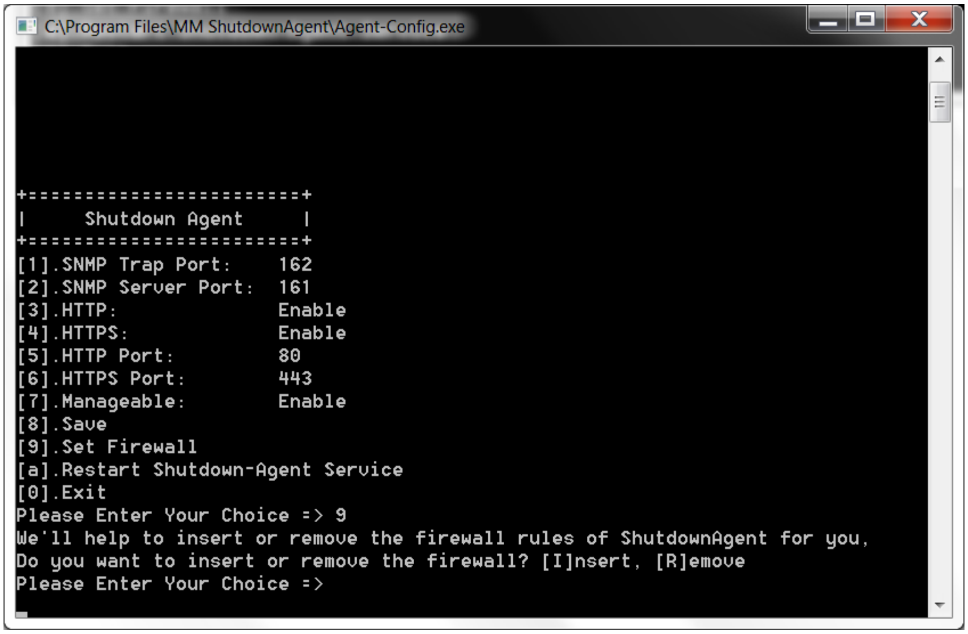
7. VMWare ESXi4 Setup for the ShutdownAgent

Before installing the ShutdownAgent in the ESXi4 server, transmit the ShutdownAgent setup file to the ESX server through SFTP by FileZilla FTP Client or another SFTP client then login to the ESX server by the local console or through your SSH client (such as Putty). Follow section 2.2 for the Linux Installation/Uninstallation. See Chapter 3 for the Console Configuration.

7.1 Configure the Firewall for ESXi 4

Run the /usr/local/upsagent/configure

Select [9] to configure the firewall for the ShutdownAgent.



```
+=======================+
|     Shutdown Agent    |
+=======================+
[1].SNMP Trap Port:    162
[2].SNMP Server Port:  161
[3].HTTP:              Enable
[4].HTTPS:             Enable
[5].HTTP Port:         80
[6].HTTPS Port:        443
[7].Manageable:        Enable
[8].Save
[9].Set Firewall
[a].Restart Shutdown-Agent Service
[0].Exit
Please Enter Your Choice => 9
We'll help to insert or remove the firewall rules of ShutdownAgent for you.
Do you want to insert or remove the firewall? [I]nsert, [R]emove
Please Enter Your Choice =>
```

7.2 Install VMware Tools for the Guest OS

To shutdown the guest OS from ESXi server, install the VMware tools on all of the guest OSes to perform the shutdown properly.

For Windows OS:

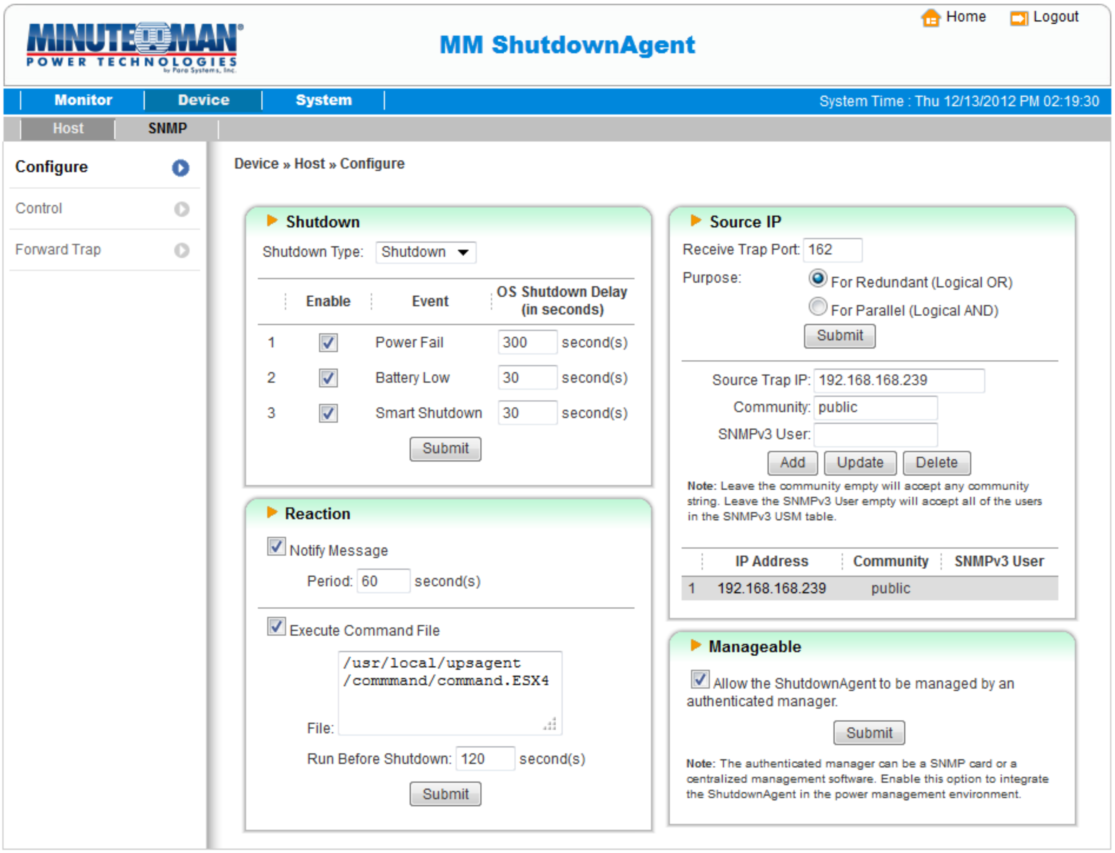
Select the following menu Guest → Install/Upgrade VMware Tools

7.3 Configure the ShutdownAgent for ESXi4

Enter the estimated time for all of the guest OSes that operate on the ESXi4 server to properly shutdown.

1. Login to the web interface of the ShutdownAgent. The account level should be equal to or greater than the device manager.
2. Goto the Device → Host → Configure web page and fill in the estimated time in the **Run Before Shutdown** field of the **Reaction** group.
3. Enter **/user/local/upsagent/command/command.ESX4** script file for ESXi 4 to shutdown the guest OSes. Then check the Execute Command File checkbox to enable the shutdown of the guest OSes.

4. Press the **Submit** button to update your changes.



System Time : Thu 12/13/2012 PM 02:19:30

Device » Host » Configure

Shutdown

Shutdown Type: Shutdown

	Enable	Event	OS Shutdown Delay (in seconds)
1	☑	Power Fail	300 second(s)
2	☑	Battery Low	30 second(s)
3	☑	Smart Shutdown	30 second(s)

Reaction

☑ Notify Message

Period: 60 second(s)

☑ Execute Command File

File: /usr/local/upsagent/command/command.ESX4

Run Before Shutdown: 120 second(s)

Source IP

Receive Trap Port: 162

Purpose: ● For Redundant (Logical OR) ○ For Parallel (Logical AND)

Source Trap IP: 192.168.168.239

Community: public

SNMPv3 User:

Note: Leave the community empty will accept any community string. Leave the SNMPv3 User empty will accept all of the users in the SNMPv3 USM table.

	IP Address	Community	SNMPv3 User
1	192.168.168.239	public	

Manageable

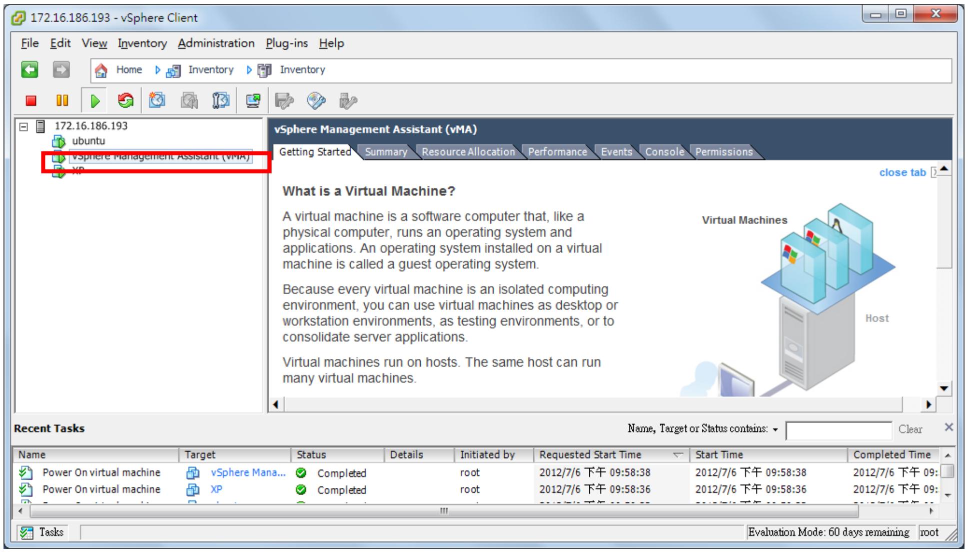
☑ Allow the ShutdownAgent to be managed by an authenticated manager.

Note: The authenticated manager can be a SNMP card or a centralized management software. Enable this option to integrate the ShutdownAgent in the power management environment.

]

8. VMWare ESXi5 Setup for the ShutdownAgent

Before installing the ShutdownAgent for the ESXi5, you have to install the **vMA 5(vSphere Management Assistant 5)** and make sure the **VMWare tools** is installed on all of the guest OSes. Then transmit the ShutdownAgent setup file to the vMA server through SFTP by FileZilla FTP Client or another SFTP client then login to the vMA server by the local console or through a SSH client (such as Putty). Follow section 2.2 For Linux Installation/Uninstallation. See Chapter 3 for the Console Configuration.


172.16.186.193 - vSphere Client
File Edit View Inventory Administration Plug-ins Help
Home
Inventory
Inventory
172.16.186.193
ubuntu
vSphere Management Assistant (vMA)
XP
vSphere Management Assistant (vMA)
Getting Started
Summary
Resource Allocation
Performance
Events
Console
Permissions
close tab
Virtual Machines
Host
Recent Tasks
Name, Target or Status contains:
Clear
Tasks
Evaluation Mode: 60 days remaining
root

What is a Virtual Machine?

A virtual machine is a software computer that, like a physical computer, runs an operating system and applications. An operating system installed on a virtual machine is called a guest operating system.

Because every virtual machine is an isolated computing environment, you can use virtual machines as desktop or workstation environments, as testing environments, or to consolidate server applications.

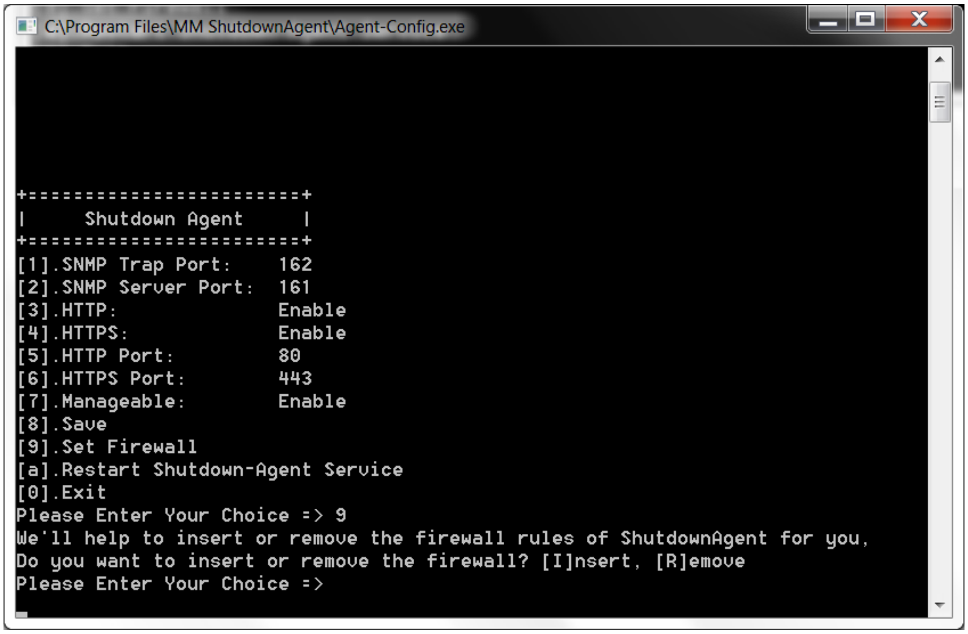
Virtual machines run on hosts. The same host can run many virtual machines.

Name	Target	Status	Details	Initiated by	Requested Start Time	Start Time	Completed Time
Power On virtual machine	vSphere Mana...	Completed		root	2012/7/6 下午 09:58:38	2012/7/6 下午 09:58:38	2012/7/6 下午 09:
Power On virtual machine	XP	Completed		root	2012/7/6 下午 09:58:36	2012/7/6 下午 09:58:36	2012/7/6 下午 09:

8.1 Configure the Firewall for vMA

Run the /usr/local/upsagent/configure

Select [9] to configure the firewall for the ShutdownAgent.



```
+=======================+
|     Shutdown Agent    |
+=======================+
[1].SNMP Trap Port:    162
[2].SNMP Server Port:  161
[3].HTTP:              Enable
[4].HTTPS:             Enable
[5].HTTP Port:         80
[6].HTTPS Port:        443
[7].Manageable:        Enable
[8].Save
[9].Set Firewall
[a].Restart Shutdown-Agent Service
[0].Exit
Please Enter Your Choice => 9
We'll help to insert or remove the firewall rules of ShutdownAgent for you,
Do you want to insert or remove the firewall? [I]nsert, [R]emove
Please Enter Your Choice =>
```

8.2 Install VMware Tools for the Guest OS

To shutdown the guest OS from ESXi5 server, install the VMware tools on all of the guest OSes to perform the shutdown.

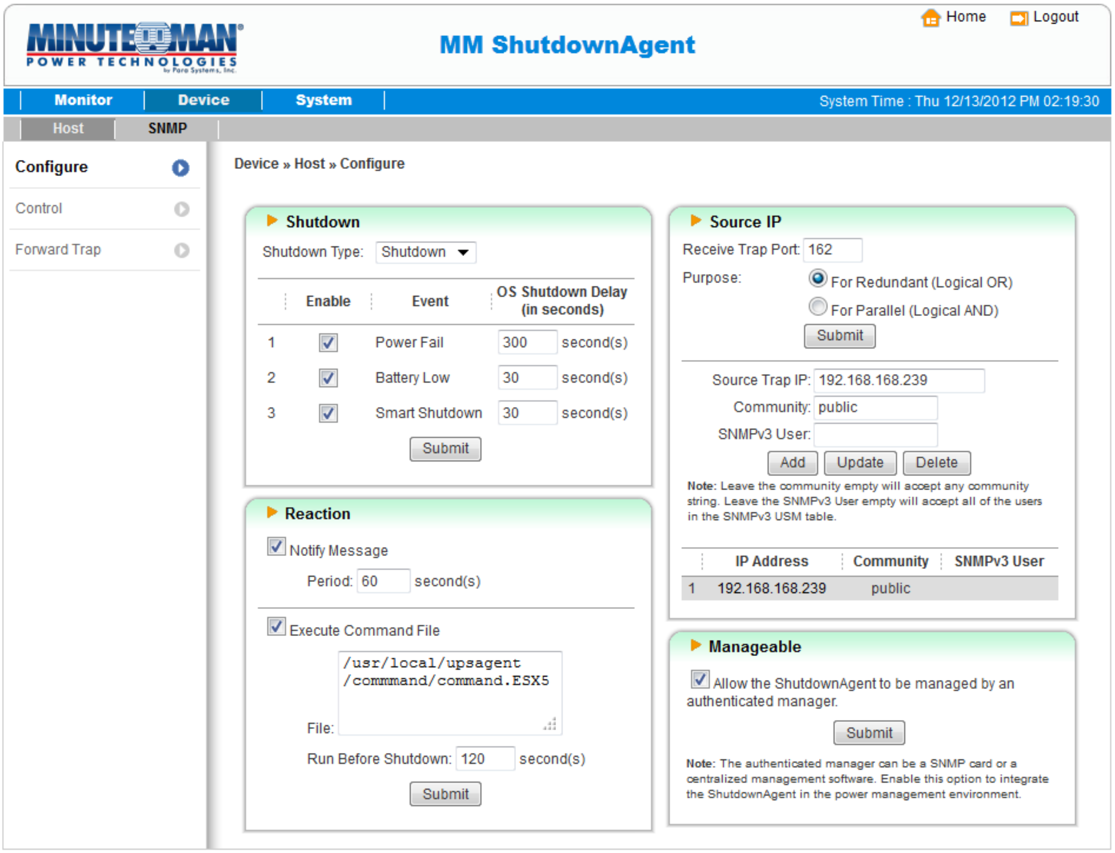
For Windows OS:

Select the following menu Guest → Install/Upgrade VMware Tools

8.3 Configure the ShutdownAgent for ESXi5

Enter the estimate time for all of the guest OSes that operate on the ESXi5 server to properly shutdown.

1. Login to the web interface of the ShutdownAgent. The account level should be equal to or greater than the device manager.
2. Goto the Device → Host → Configure web page and fill in the estimated time in the **Run Before Shutdown** field of the **Reaction** group.
3. Enter **/user/local/upsagent/command/command.ESX5** script file for ESXi5 to shutdown the guest OSes. Then check the Execute Command File checkbox to enable the shutdown of the guest OSes.
4. Press the **Submit** button to update your changes.



System Time : Thu 12/13/2012 PM 02:19:30

Device » Host » Configure

Shutdown Type: Shutdown

	Enable	Event	OS Shutdown Delay (in seconds)
1	☑	Power Fail	300 second(s)
2	☑	Battery Low	30 second(s)
3	☑	Smart Shutdown	30 second(s)

☑ Notify Message

Period: 60 second(s)

☑ Execute Command File

File: /usr/local/upsagent /commmand/command.ESX5

Run Before Shutdown: 120 second(s)

Receive Trap Port: 162

Purpose: ● For Redundant (Logical OR) ○ For Parallel (Logical AND)

Source Trap IP: 192.168.168.239

Community: public

SNMPv3 User:

Note: Leave the community empty will accept any community string. Leave the SNMPv3 User empty will accept all of the users in the SNMPv3 USM table.

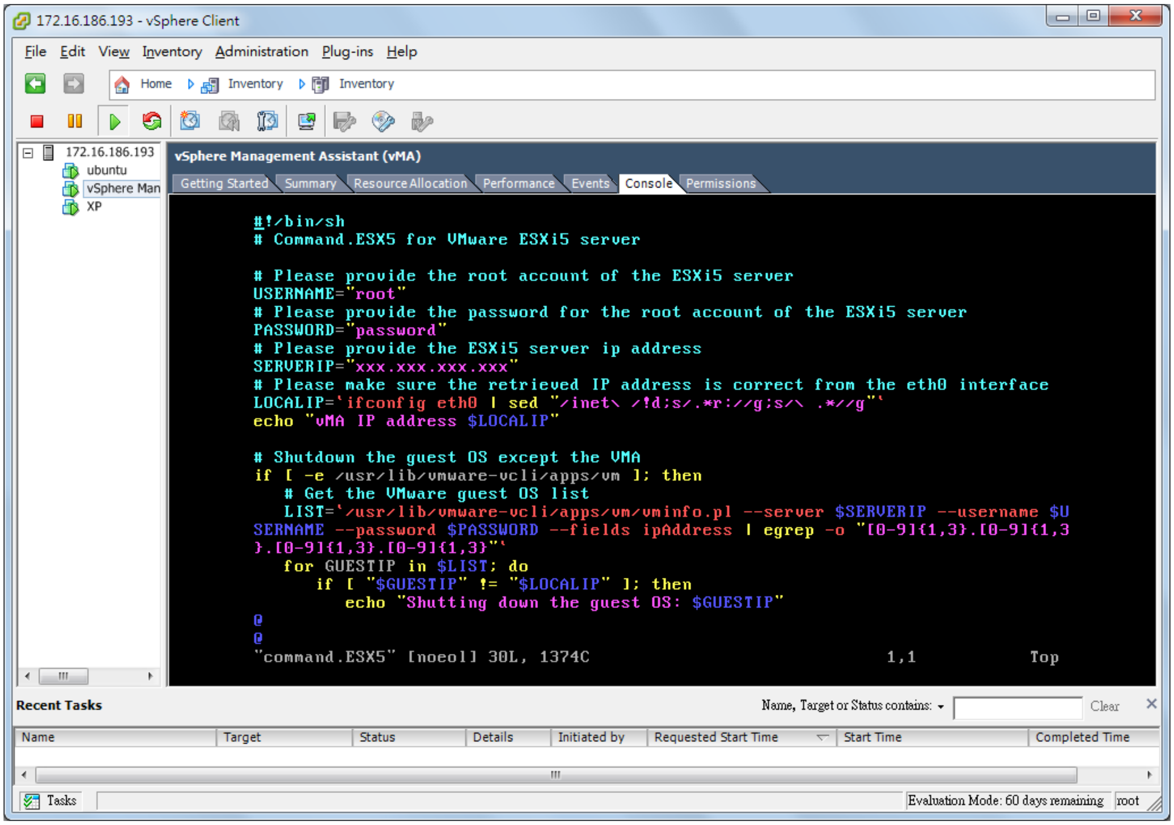
	IP Address	Community	SNMPv3 User
1	192.168.168.239	public	

☑ Allow the ShutdownAgent to be managed by an authenticated manager.

Note: The authenticated manager can be a SNMP card or a centralized management software. Enable this option to integrate the ShutdownAgent in the power management environment.

8.4 Modify the Command.ESX5

The command.ESX5 script needs to be configured to provide the user name, password for the vMA to communicate with the ESXi5 server. Login to the vMA server with the root privilege and open the following script file with a text edit program:
/usr/local/upsagent/command/command.ESX5.



```
#!/bin/sh
# Command.ESX5 for VMware ESXi5 server

# Please provide the root account of the ESXi5 server
USERNAME="root"
# Please provide the password for the root account of the ESXi5 server
PASSWORD="password"
# Please provide the ESXi5 server ip address
SERVERIP="xxx.xxx.xxx.xxx"
# Please make sure the retrieved IP address is correct from the eth0 interface
LOCALIP=`ifconfig eth0 | sed "/inet\ /!d;s/.*r://g;s/\ .*//g"`
echo "vMA IP address $LOCALIP"

# Shutdown the guest OS except the VMA
if [ -e /usr/lib/vmware-vcli/apps/vm ]; then
   # Get the VMware guest OS list
   LIST=`/usr/lib/vmware-vcli/apps/vm/vminfo.pl --server $SERVERIP --username $U
SERNAME --password $PASSWORD --fields ipAddress | egrep -o "[0-9]{1,3}.[0-9]{1,3
}.[0-9]{1,3}.[0-9]{1,3}"`
   for GUESTIP in $LIST; do
      if [ "$GUESTIP" != "$LOCALIP" ]; then
         echo "Shutting down the guest OS: $GUESTIP"
@
@
"command.ESX5" [noeol] 30L, 1374C                             1,1           Top
```

USERNAME: The root account of the ESXi5 server.
PASSWORD: The password for the root account of the ESXi5 server.
SERVERIP: The IP address of the ESXi5 server.
LOCALIP: The IP address of the vMA server.
Normally you have to provide the root password for the PASSWORD and the ESXi5 server IP address for the SERVERIP. The script gets the vMA IP address from the eth0 interface automatically. If it is incorrect for your network configuration change it to the interface which you have created.

9. XenServer Setup for the ShutdownAgent

To install the ShutdownAgent in theCitrix XenServer, see section 2.2 for the Linux Installation/Uninstallation. To configure the basic networking parameters including the Xen firewall, see Chapter 3 Console Configuration.

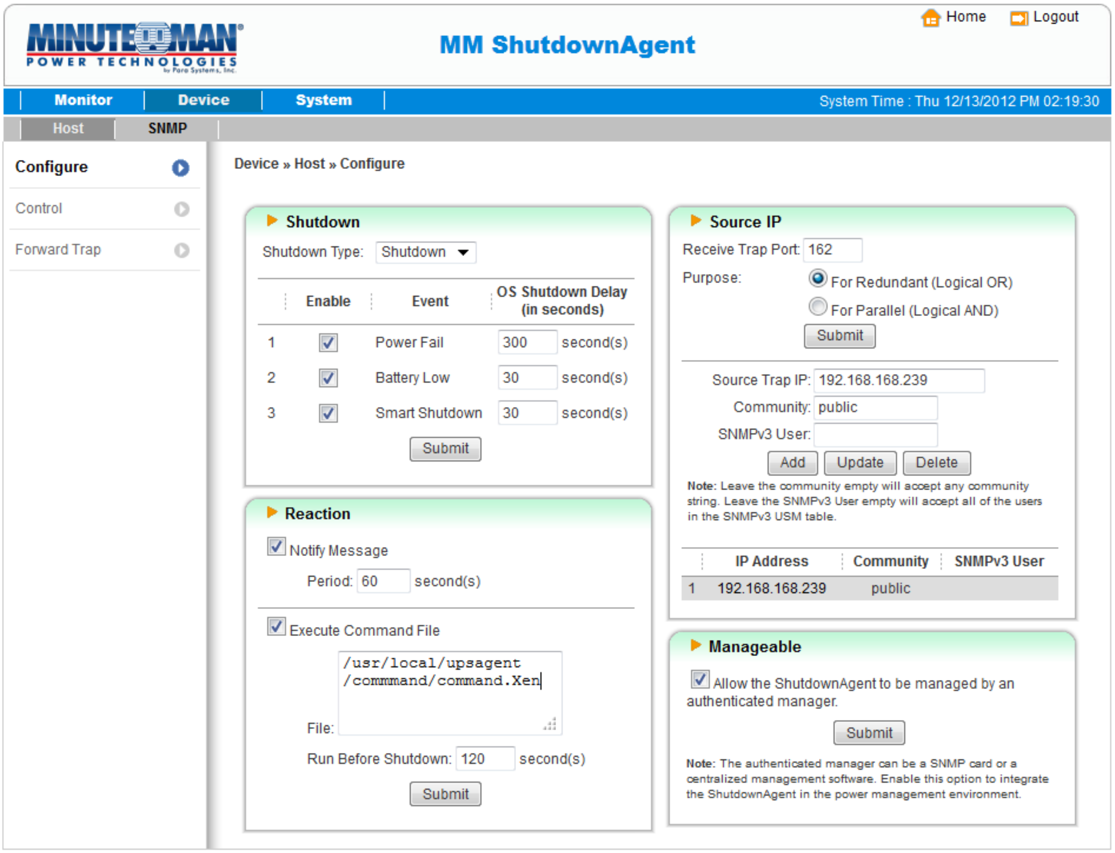
9.1 Install PV driver for the Guest OS

To shutdown the guest OS from XenServer, you need to install the PV driver for all of the guest OSes.

9.2 Configure the ShutdownAgent for Xen

Enter the estimated time for all of the guest OSes that operate on the XenServer to properly shutdown.

1. Login to the web interface of the ShutdownAgent. The account level should be equal to or greater than the device manager.
2. Goto the Device → Host → Configure web page and fill in the estimated time in the **Run Before Shutdown** field of the **Reaction** group.
3. Enter **/user/local/upsagent/command/command.Xen** script file to shutdown the guest OSes. Then check the Execute Command File checkbox to enable the shutdown of the guest OSes.
4. Press the **Submit** button to update your changes.



System Time : Thu 12/13/2012 PM 02:19:30

Device » Host » Configure

Shutdown

Shutdown Type: Shutdown

	Enable	Event	OS Shutdown Delay (in seconds)	
1	☑	Power Fail	300	second(s)
2	☑	Battery Low	30	second(s)
3	☑	Smart Shutdown	30	second(s)

Reaction

☑ Notify Message

Period: 60 second(s)

☑ Execute Command File

File: /usr/local/upsagent/command/command.Xen

Run Before Shutdown: 120 second(s)

Source IP

Receive Trap Port: 162

Purpose: ● For Redundant (Logical OR) ○ For Parallel (Logical AND)

Source Trap IP: 192.168.168.239

Community: public

SNMPv3 User:

Note: Leave the community empty will accept any community string. Leave the SNMPv3 User empty will accept all of the users in the SNMPv3 USM table.

	IP Address	Community	SNMPv3 User
1	192.168.168.239	public	

Manageable

☑ Allow the ShutdownAgent to be managed by an authenticated manager.

Note: The authenticated manager can be a SNMP card or a centralized management software. Enable this option to integrate the ShutdownAgent in the power management environment.

10. Linux KVM Setup for the ShutdownAgent

To install the ShutdownAgent on the Linux server, see section 2.2 Installation/Uninstallation. To configure the basic networking parameters including the firewall, see Chapter 3 Console Configuration.

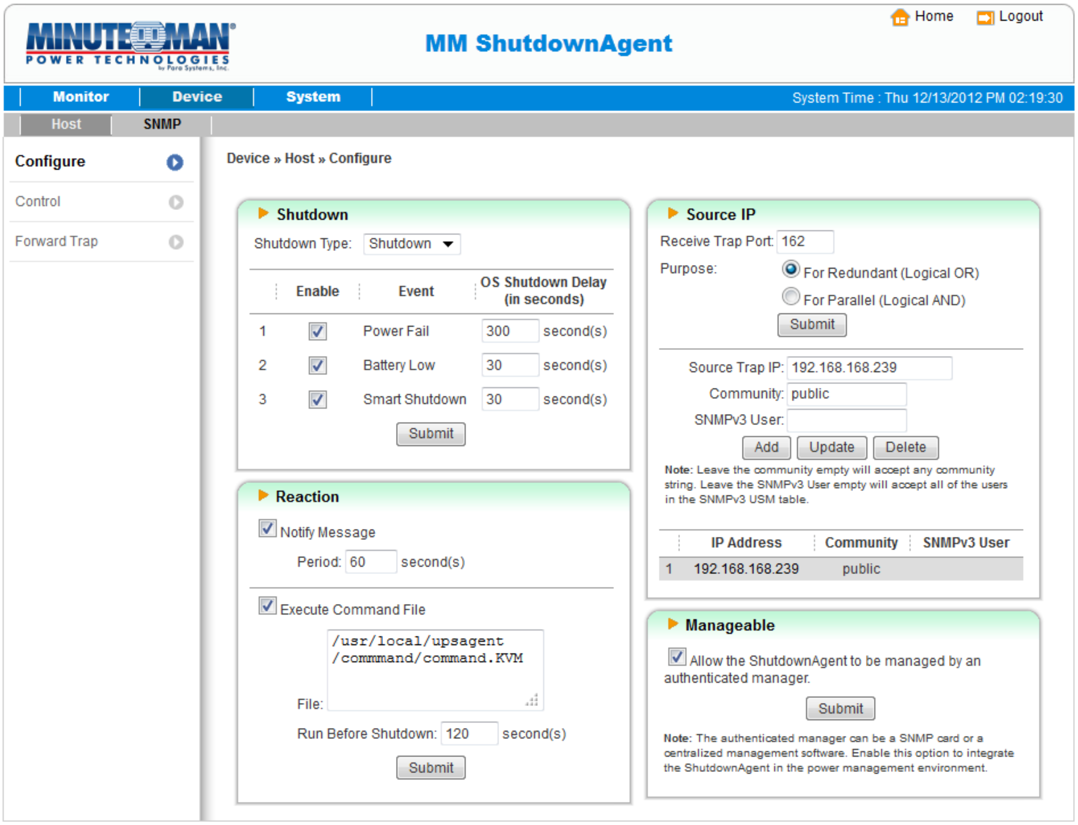
10.1 Install libvirt Tools for KVM

To shutdown the guest OS from Linux server, you have to install the libvirt. The ShutdownAgent calls the virsh to shutdown the guest OSes.

10.2 Configure the ShutdownAgent for KVM

Enter the estimated time for all of the guest OSes that operate on the KVM server to properly shutdown.

1. Login to the web interface of the ShutdownAgent. The account level should be equal to or greater than the device manager.
2. Goto the Device → Host → Configure web page and fill in the estimated time in the **Run Before Shutdown** field of the **Reaction** group.
3. Enter **/user/local/upsagent/command/command.KVM** script file to shutdown the guest OSes. Then check the Execute Command File checkbox to enable the shutdown of the guest OSes.
4. Press the **Submit** button to update your changes.



System Time : Thu 12/13/2012 PM 02:19:30

Device » Host » Configure

Shutdown

Shutdown Type: Shutdown

	Enable	Event	OS Shutdown Delay (in seconds)
1	☑	Power Fail	300 second(s)
2	☑	Battery Low	30 second(s)
3	☑	Smart Shutdown	30 second(s)

Reaction

☑ Notify Message

Period: 60 second(s)

☑ Execute Command File

File: /usr/local/upsagent /commmand/command.KVM

Run Before Shutdown: 120 second(s)

Source IP

Receive Trap Port: 162

Purpose: ● For Redundant (Logical OR) ○ For Parallel (Logical AND)

Source Trap IP: 192.168.168.239

Community: public

SNMPv3 User:

Note: Leave the community empty will accept any community string. Leave the SNMPv3 User empty will accept all of the users in the SNMPv3 USM table.

	IP Address	Community	SNMPv3 User
1	192.168.168.239	public	

Manageable

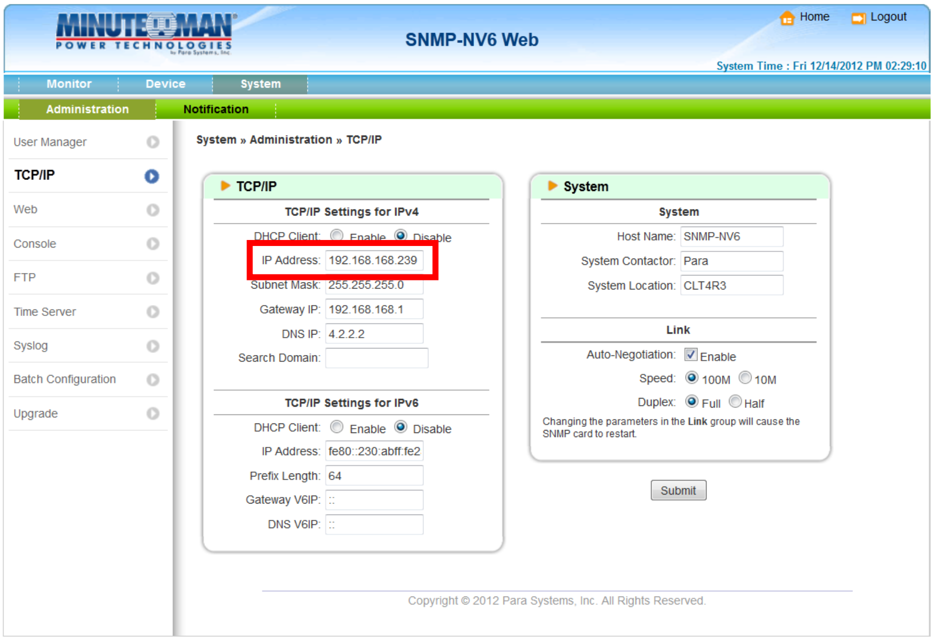
☑ Allow the ShutdownAgent to be managed by an authenticated manager.

Note: The authenticated manager can be a SNMP card or a centralized management software. Enable this option to integrate the ShutdownAgent in the power management environment.

11. Working with the SNMP Card

11.1 SNMP-NV6 Card

1. Open a web browser and connect to the SNMP-NV6 card.
2. Record the IP address from the System Configuration web page.



System Time : Fri 12/14/2012 PM 02:29:10

System » Administration » TCP/IP

TCP/IP

TCP/IP Settings for IPv4

DHCP Client: ○ Enable ● Disable
IP Address: 192.168.168.239
Subnet Mask: 255.255.255.0
Gateway IP: 192.168.168.1
DNS IP: 4.2.2.2
Search Domain:

TCP/IP Settings for IPv6

DHCP Client: ○ Enable ● Disable
IP Address: fe80::230:abff:fe2
Prefix Length: 64
Gateway V6IP: ::
DNS V6IP: ::

System

System

Host Name: SNMP-NV6
System Contactor: Para
System Location: CLT4R3

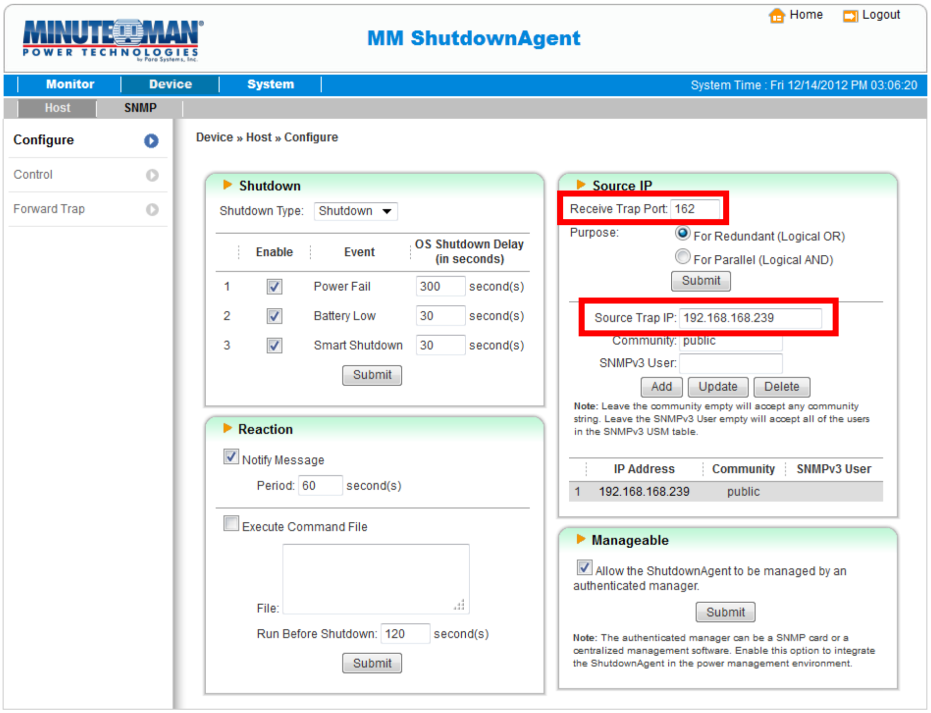
Link

Auto-Negotiation: ☑ Enable
Speed: ● 100M ○ 10M
Duplex: ● Full ○ Half

Changing the parameters in the **Link** group will cause the SNMP card to restart.

Copyright © 2012 Para Systems, Inc. All Rights Reserved.

3. Login to the ShutdownAgent and add the SNMP-NV6 card's IP address and the trap port to receive the SNMP trap from the SNMP-NV6 card.



System Time : Fri 12/14/2012 PM 03:06:20

Device » Host » Configure

Shutdown

Shutdown Type: Shutdown

	Enable	Event	OS Shutdown Delay (in seconds)	
1	☑	Power Fail	300	second(s)
2	☑	Battery Low	30	second(s)
3	☑	Smart Shutdown	30	second(s)

Reaction

☑ Notify Message
Period: 60 second(s)

☐ Execute Command File
File:
Run Before Shutdown: 120 second(s)

Source IP

Receive Trap Port: 162
Purpose: ● For Redundant (Logical OR)
○ For Parallel (Logical AND)

Source Trap IP: 192.168.168.239
Community: public
SNMPv3 User:

Note: Leave the community empty will accept any community string. Leave the SNMPv3 User empty will accept all of the users in the SNMPv3 USM table.

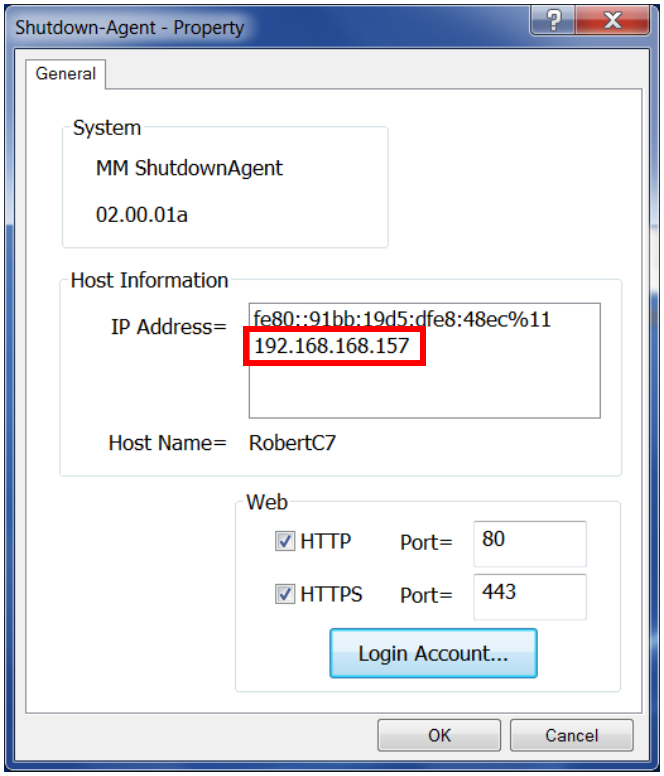
	IP Address	Community	SNMPv3 User
1	192.168.168.239	public	

Manageable

☑ Allow the ShutdownAgent to be managed by an authenticated manager.

Note: The authenticated manager can be a SNMP card or a centralized management software. Enable this option to integrate the ShutdownAgent in the power management environment.

4. Open the ShutdownAgent's property window from the Windows task bar to get the IP address of the server.



System

MM ShutdownAgent

02.00.01a

Host Information

IP Address= fe80::91bb:19d5:dfe8:48ec%11
192.168.168.157

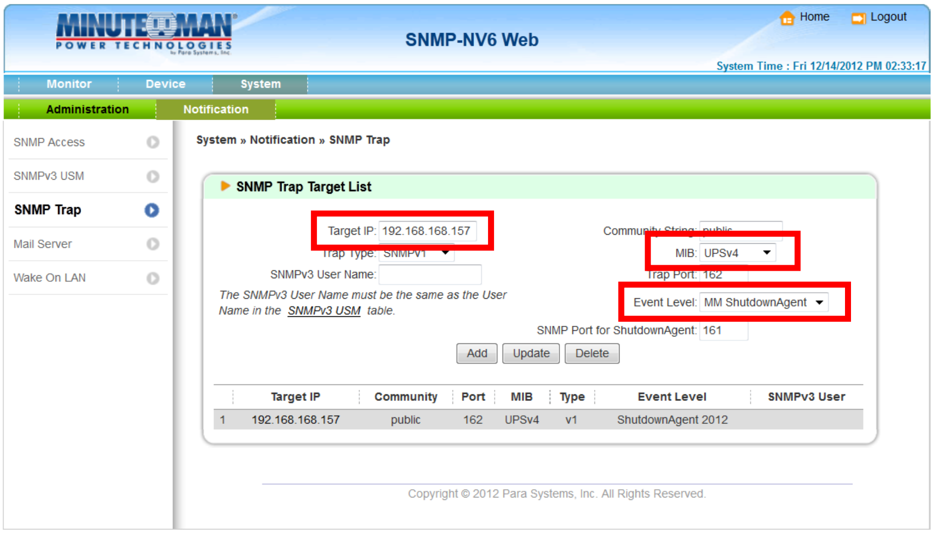
Host Name= RobertC7

Web

☑ HTTP Port= 80

☑ HTTPS Port= 443

5. Go back to the SNMP-NV6 card and add the IP address of ShutdownAgent to the SNMP Trap table. Select the UPSV4 as the Trap MIB and the MM ShutdownAgent for the Event Level.



System Time : Fri 12/14/2012 PM 02:33:17

System » Notification » SNMP Trap

SNMP Trap Target List

Target IP: 192.168.168.157

Trap Type: SNMPV1

SNMPv3 User Name:

The SNMPv3 User Name must be the same as the User Name in the SNMPv3 USM table.

Community String: public

MIB: UPSv4

Trap Port: 162

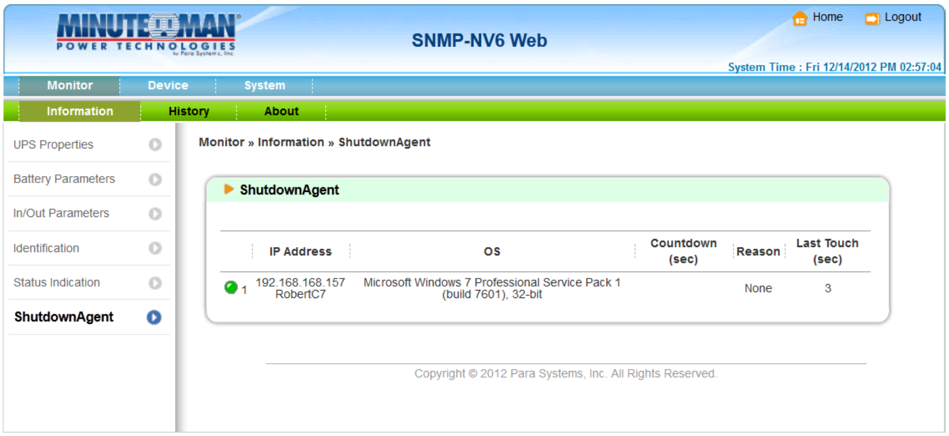
Event Level: MM ShutdownAgent

SNMP Port for ShutdownAgent: 161

	Target IP	Community	Port	MIB	Type	Event Level	SNMPv3 User
1	192.168.168.157	public	162	UPSv4	v1	ShutdownAgent 2012	

Copyright © 2012 Para Systems, Inc. All Rights Reserved.

6. If you enable the Manageable option in the ShutdownAgent then you can monitor the status of the ShutdownAgents from the SNMP-NV6 card (Monitor >> Information >> ShutdownAgent).



System Time : Fri 12/14/2012 PM 02:57:04

	IP Address	OS	Countdown (sec)	Reason	Last Touch (sec)
● 1	192.168.168.157 RobertC7	Microsoft Windows 7 Professional Service Pack 1 (build 7601), 32-bit		None	3

Copyright © 2012 Para Systems, Inc. All Rights Reserved.

11.2 SNMP-NET Card

1. Open a web browser and connect to the SNMP-NET Card.
2. Record the IP address and SNMP Trap port on the System Configuration web page.
3. Add the SNMP-NET card’s IP address and the Trap port to the ShutdownAgent’s Device >> Host >> Configure page.
4. Get the ShutdownAgent’s IP address from the property dialog box.
5. Add the ShutdownAgent’s IP address to the SNMP Trap table in the SNMP-NET Card.
6. Select the Information for the Event Level and MMv4 as the Trap MIB Type.