



# **MM ShutdownAgent**

## **User Manual**

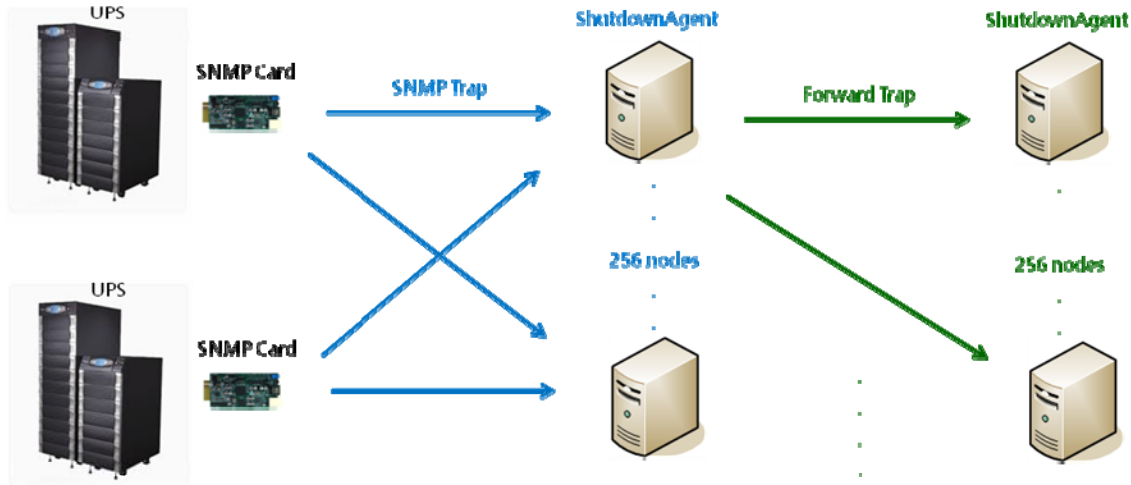
# Contents

<b>1. Overview.....</b>	<b>3</b>
1.1 Features .....	3
1.2 OS Support.....	3
<b>2. Installation / Uninstall .....</b>	<b>4</b>
2.1 For Windows System .....	4
2.1.1 Installation Process .....	4
2.1.2 Uninstall Process.....	8
2.2 For Linux System .....	8
2.2.1 Installation Process .....	8
2.2.2 Uninstall Process.....	9
<b>3. Console Configuration .....</b>	<b>10</b>
3.1 Console Menu .....	10
<b>4. Operation in Windows.....</b>	<b>11</b>
4.1 Web Monitor .....	11
4.2 Property.....	12
4.3 Show Countdown .....	13
4.4 Cancel Countdown .....	13
4.5 Stop Service .....	13
<b>5. Web Interface .....</b>	<b>14</b>
5.1 Run a Web Browser .....	14
5.2 Monitor >> Information >> Summary.....	15
5.3 Monitor >> Information >> Event Log.....	16
5.4 Monitor >> Information >> Log Configure.....	17
5.5 Monitor >> About >> Information.....	17
5.6 Device >> Host >> Configure .....	17
5.7 Device >> Host >> Control .....	20
5.8 Device >> Host >> Forward Trap .....	20
5.9 Device >> SNMP >> SNMP Access.....	21
5.10 Device >> SNMP >> SNMPv3 USM.....	21
5.11 System >> Administration >> Information.....	22
5.12 System >> Administration >> Login User .....	22
5.13 System >> Administration >> Web .....	23
5.14 System >> Administration >> Batch Configuration .....	24
<b>6. 2008 Server Core Setup for the ShutdownAgent.....</b>	<b>25</b>
<b>7. VMWare ESXi4 Setup for the ShutdownAgent.....</b>	<b>26</b>
7.1 Configure the Firewall for ESXi 4 .....	26
7.2 Install VMware Tools for the Guest OS .....	26
7.3 Configure the ShutdownAgent for ESXi4 .....	26
<b>8. VMWare ESXi5 Setup for the ShutdownAgent.....</b>	<b>28</b>

8.1 Configure the Firewall for vMA .....	28
8.2 Install VMware Tools for the Guest OS .....	29
8.3 Configure the ShutdownAgent for ESXi5 .....	29
8.4 Modify the Command.ESX5 .....	30
<b>9. XenServer Setup for the ShutdownAgent .....</b>	<b>31</b>
9.1 Install PV driver for the Guest OS .....	31
9.2 Configure the ShutdownAgent for Xen .....	31
<b>10. Linux KVM Setup for the ShutdownAgent .....</b>	<b>32</b>
10.1 Install libvirt Tools for KVM .....	32
10.2 Configure the ShutdownAgent for KVM.....	32
<b>11. Working with the SNMP Card .....</b>	<b>33</b>
11.1 SNMP-NV6 Card .....	33
11.2 SNMP-NET Card.....	35

# 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

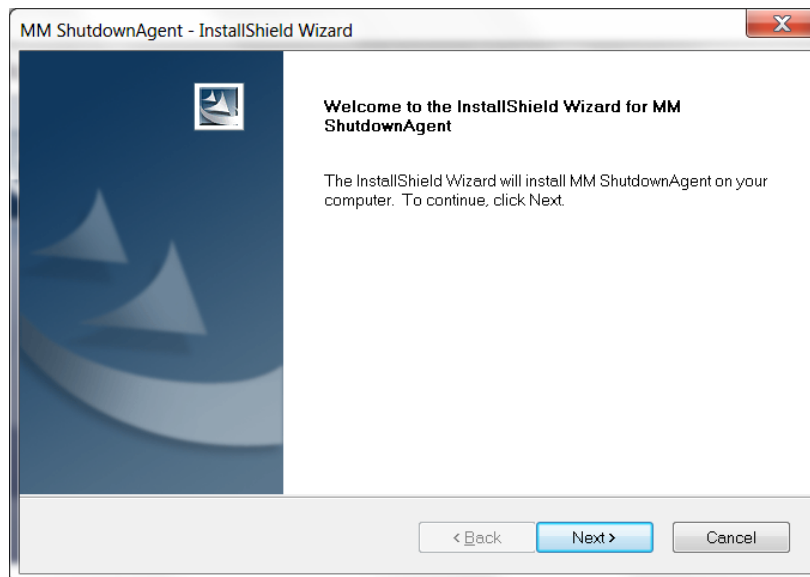
## 2. Installation / Uninstall

### 2.1 For Windows System

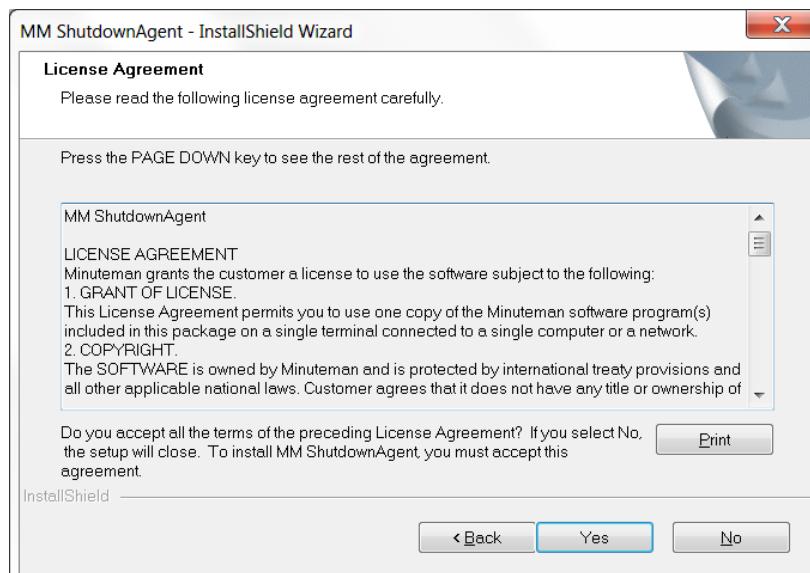
There are two setup programs: MM-ShutdownAgent-Setup(win32).exe and MM-ShutdownAgent-Setup(x64).exe. One is for 32 bit Windows operating system and the other one is for 64 bit Windows environment.

#### 2.1.1 Installation Process

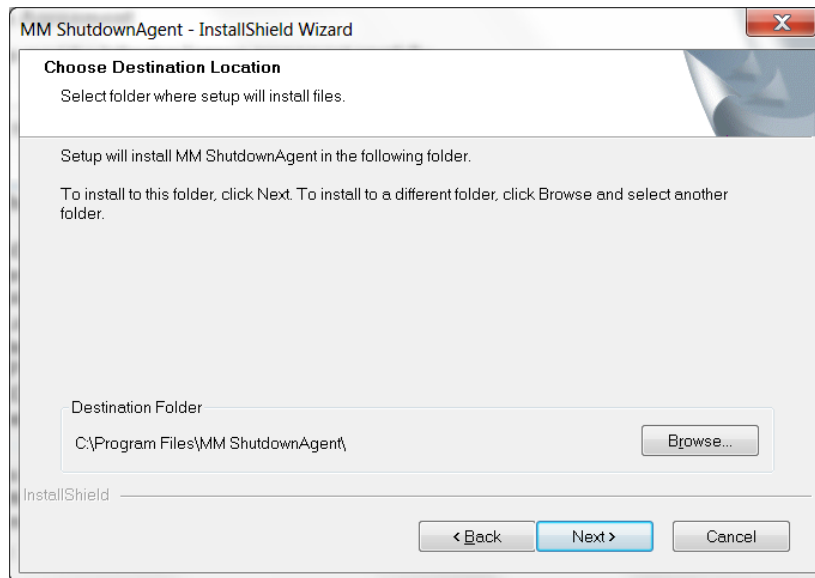
1. Execute the MM-ShutdownAgent-Setup (xxx).exe to run the setup program.
2. The welcome page will be displayed, press the “Next” button to continue with the installation.



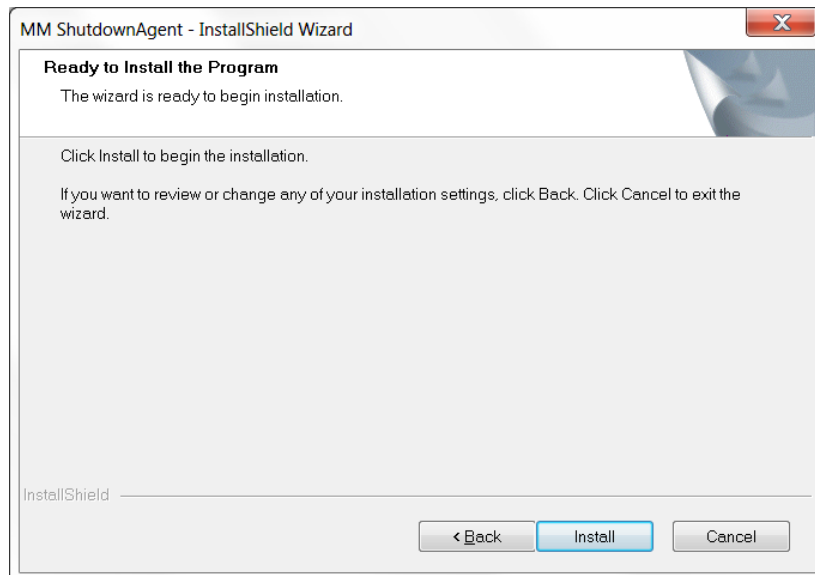
3. Press the “Yes” button to accept the license agreement and continue with the installation.



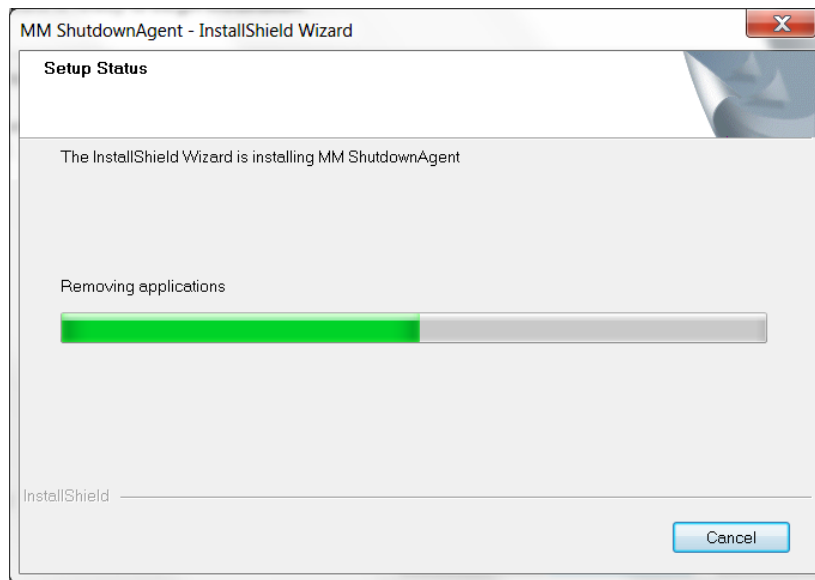
4. Select a different location by using the Browse button or press the “Next” button to install the software in the default location.



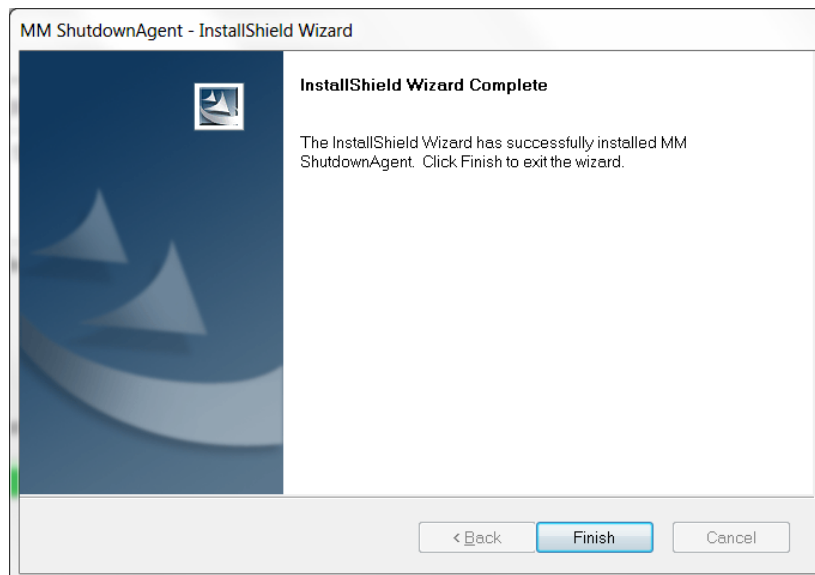
5. Press the “Install” button to start installing the software to the designated location.



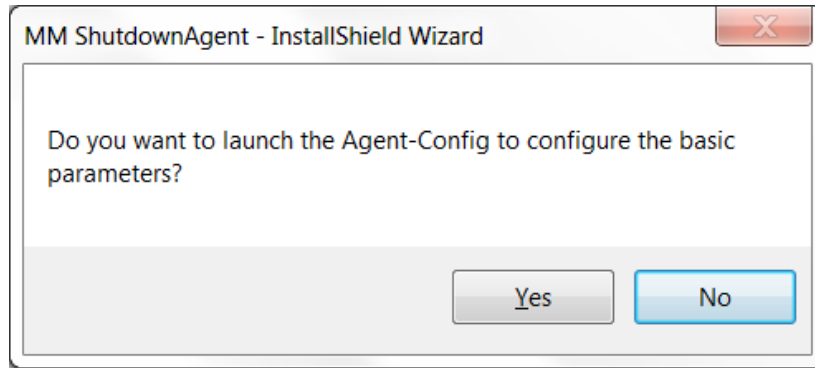
6. The Installation is in process.



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



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.



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.

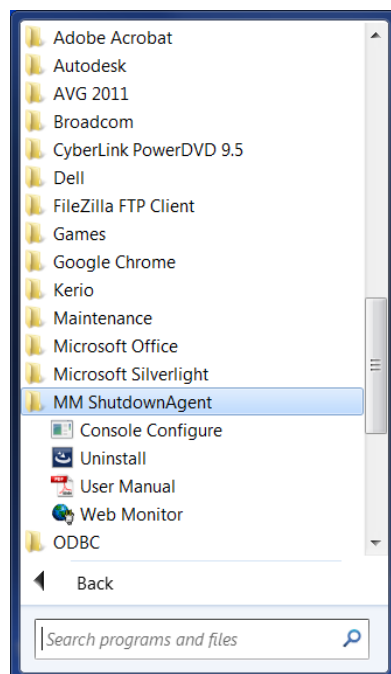
After finishing the installation, the setup program will create a MM ShutdownAgent association with the following shortcuts:

**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.

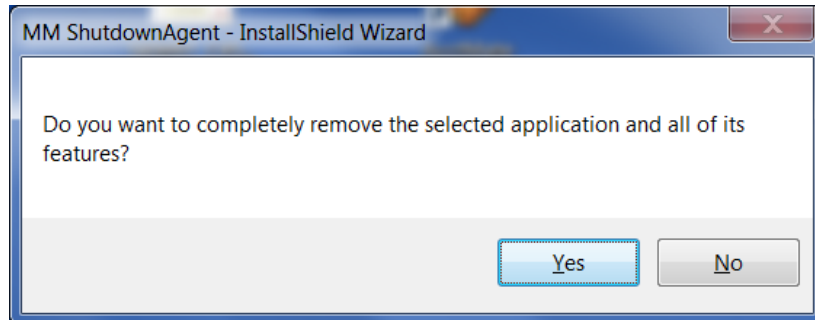
**Web Monitor:** The user interface of MM ShutdownAgent used to monitor and configure the software.



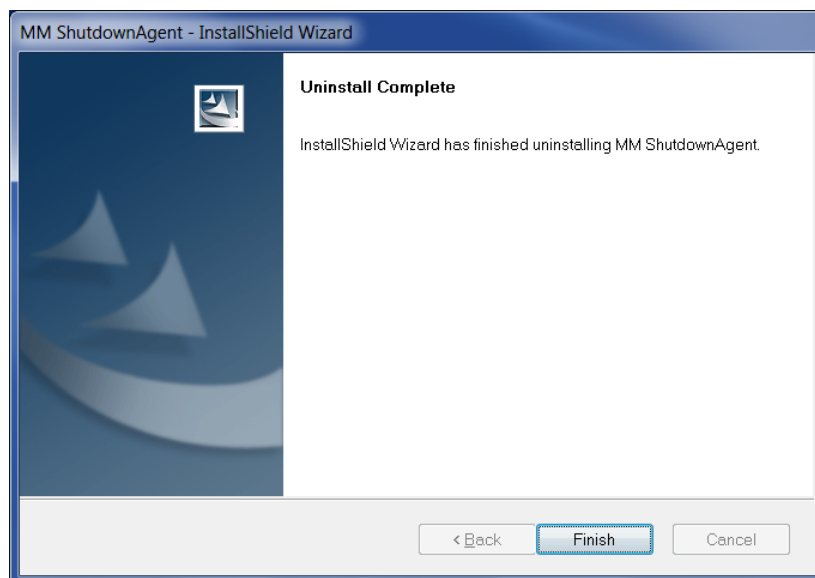


## 2.1.2 Uninstall Process

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.



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



## 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

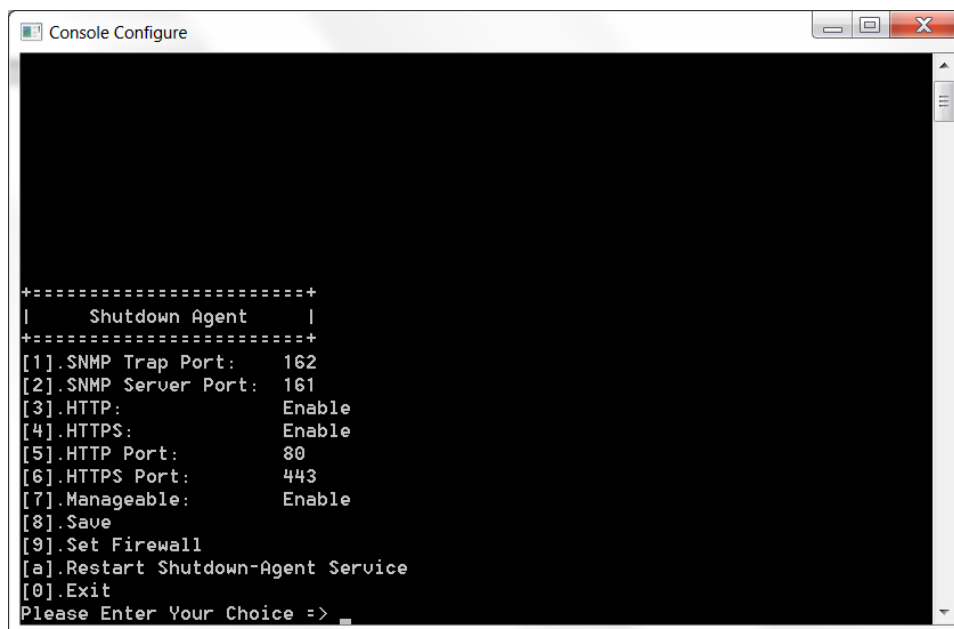
1. Login to the Linux system and change to the root account:  
su root
2. Change your working directory to /usr/local/upsagent:  
cd /usr/local/upsagent
3. Run the uninstall script to remove the MM ShutdownAgent:  
./uninstall
4. Press 'y' to start the uninstall process.

### 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”



```

Console 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

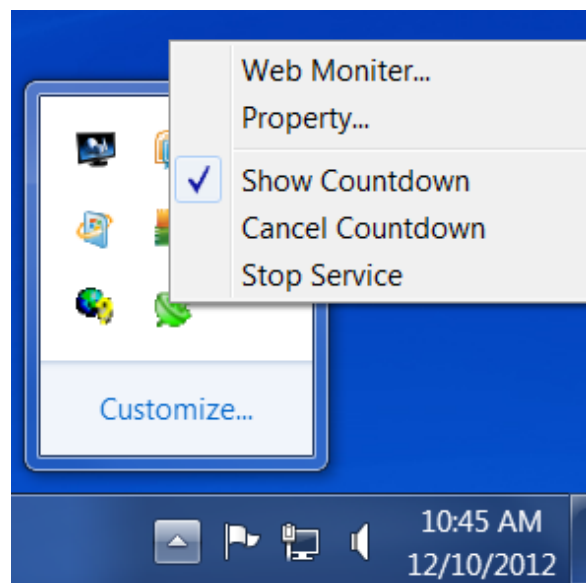
No.	Function	Description	Default
1.	SNMP Trap Port	The UDP port to listen for the SNMP trap	162
2.	SNMP Server Port	The UDP port for replying to get/set commands	161
3.	HTTP	Enable or disable the HTTP protocol	Enable
4.	HTTPS	Enable or disable the HTTPS protocol	Enable
5.	HTTP Port	The TCP port for HTTP	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.



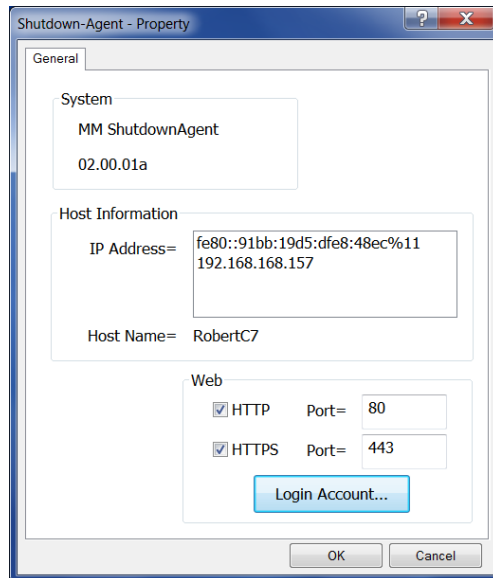
### 4.1 Web Monitor

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.



### 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.

	<b>Account</b>	<b>Password</b>
Administrator	admin	password
Device Manager	device	password
Read Only User	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.

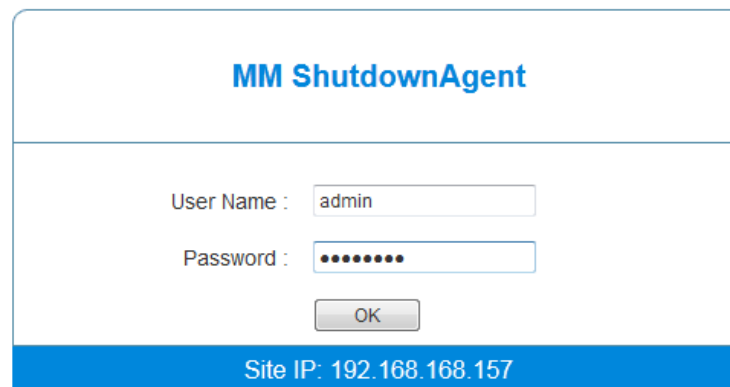
The ShutdownAgent allows a maximum of 16 users to login at the same time.

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 :

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.

The screenshot shows the MM ShutdownAgent web interface. The top navigation bar includes 'Monitor', 'Device', and 'System' tabs, with 'System' selected. The system time is 'Tue 12/11/2012 AM 11:12:41'. The main content area is titled 'Monitor » Information » Summary' and contains several sections:

- 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: [Progress bar]
- SNMP Trap Source IP List:** Purpose: For Redundant (Logical OR). Table with columns: Source IP, UPS Health, Current Event. Row 1: 192.168.168.239, Normal.
- Last 5 Event Log:** Table with columns: Source IP, Date/Time, Event Level, Event Description.
 

	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.

The screenshot shows the MM ShutdownAgent web interface. The top navigation bar includes 'Monitor', 'Device', and 'System' tabs, with 'Monitor' selected. The system time is displayed as 'Tue 12/11/2012 AM 11:17:26'. The main content area is titled 'Monitor » Information » Event Log » Page1'. On the left, there is a sidebar with 'Event Log' selected. The main event log area has a 'Download All' button and a date filter set to 'From 12/11/2012 To 12/11/2012'. The event log table is as follows:

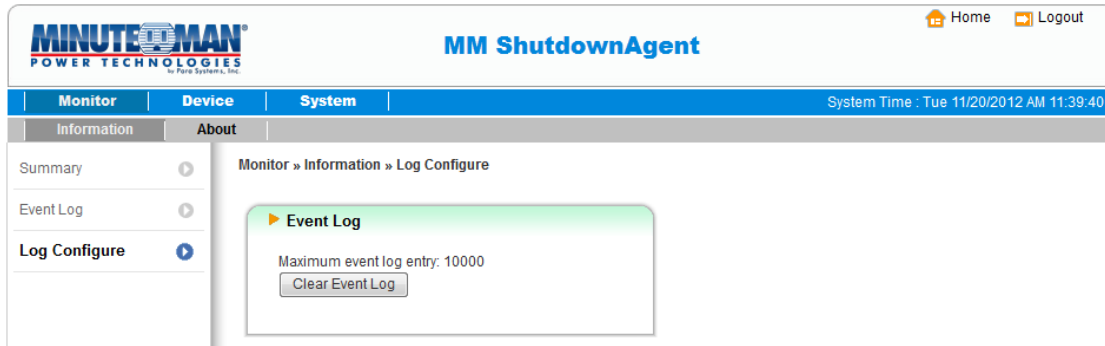
IP Address	Date	Time	Level	Event Log
192.168.168.239	12/11/2012	11:11:23	Information	Power restore
192.168.168.239	12/11/2012	11:11:03	Warning	Power fail
192.168.168.239	12/11/2012	11:09:20	Information	Power restore
192.168.168.239	12/11/2012	11:08:51	Warning	Power fail
	12/11/2012	11:02:03	System	Account 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.

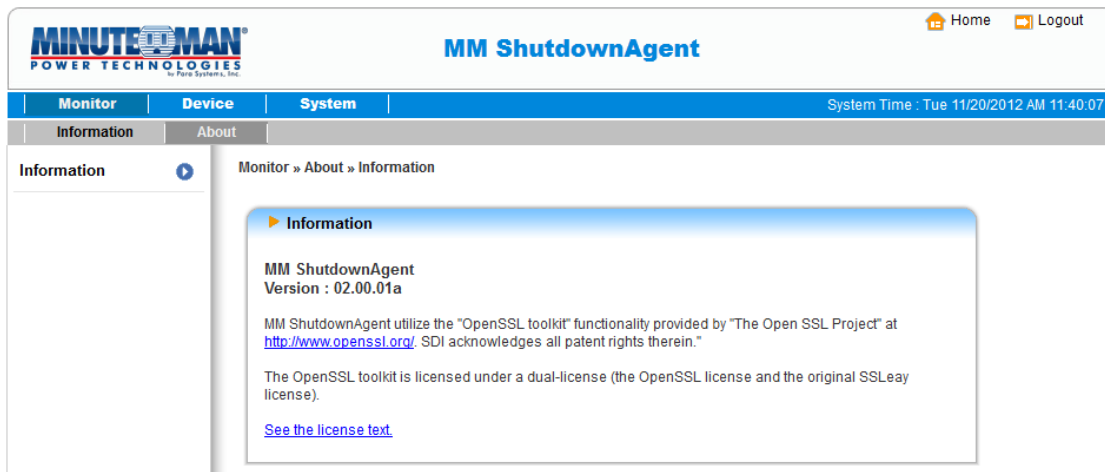
### Clear Event Log:

Click on this button to clear the event log.



## 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.



## 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.

**MINUTEMAN**  
POWER TECHNOLOGIES  
by FORT SYSTEMS, INC.

**MM ShutdownAgent**

Home Logout

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

Host SNMP

Configure Control Forward Trap

Device » Host » Configure

**Shutdown**

Shutdown Type: Shutdown

Enable	Event	OS Shutdown Delay (in seconds)
<input checked="" type="checkbox"/>	Power Fail	300 second(s)
<input checked="" type="checkbox"/>	Battery Low	30 second(s)
<input checked="" type="checkbox"/>	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:

IP Address	Community	SNMPv3 User
1 0.0.0.0	public	

**Manageable**

Allow the ShutdownAgent to be managed by an authenticated manager.

### 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.

The screenshot shows the MM ShutdownAgent web interface. The top navigation bar includes 'Monitor', 'Device', and 'System' tabs, with 'Device' selected. The system time is 'Tue 11/20/2012 AM 11:42:57'. The main content area is titled 'Device » Host » Control'. It features two main panels:

- Control Panel:** Contains buttons for 'Cancel Countdown' and 'Pause Broadcast'. A note below states: 'Note: Selecting Pause Broadcast will stop the Broadcast messages until the next event occurs.'
- Forward Simulation Trap Panel:** Contains buttons for 'Power Fail' and 'Power Restore'. A note below states: '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.

The screenshot shows the MM ShutdownAgent web interface. The top navigation bar includes 'Monitor', 'Device', and 'System' tabs, with 'Device' selected. The system time is 'Tue 11/20/2012 AM 11:43:45'. The main content area is titled 'Device » Host » Forward Trap'. It features a 'Target IP List' section with the following configuration:

- Target IP: 192.168.168.239
- UDP Port: 162 (Default: 162)
- Buttons: Add, Update, Delete

Below the configuration is a table with the following data:

	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.

The screenshot shows the 'SNMPv1 Access Table' configuration page. The form includes fields for 'SNMP Port' (161), 'Download MIB' (ShutdownAgent), 'Access IP' (0.0.0.0), 'Community' (public), and 'Permission' (Read Only). Below the form is a table with the following data:

	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.

The screenshot shows the 'SNMPv3 USM' configuration page. The form includes fields for 'Context Name' (cn1027), 'Auth Protocol' (MD5), 'Priv Protocol' (CBC-DES), 'User Name' (manager), 'Auth Password' (\*\*\*\*\*), 'Priv Password' (\*\*\*\*\*), and 'Permission' (Read/Write). Below the form is a table with the following data:

	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.

MINUTE MAN POWER TECHNOLOGIES

MM ShutdownAgent

Home Logout

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

Administration

System » Administration » Information

Information

System Name:

System Contactor:

System Location:

Installation Date:  (MM/DD/YYYY)

Description:

Submit

## 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.

MINUTE MAN POWER TECHNOLOGIES

MM ShutdownAgent

Home Logout

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

Administration

System » Administration » Login User

User Manager

	Privilege	Account Name (16 chars max.)	Password (16 chars max.)
1	Administrator	<input type="text" value="admin"/>	<input type="password" value="....."/>
2	Device Manager	<input type="text" value="device"/>	<input type="password" value="....."/>
3	Read Only User	<input type="text" value="user"/>	<input type="password" value="....."/>

Submit

## 5.13 System >> Administration >> Web

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

The screenshot shows the MM ShutdownAgent web interface. At the top, there is a navigation bar with 'Monitor', 'Device', and 'System' tabs. The 'System' tab is active, and the page title is 'MM ShutdownAgent'. Below the navigation bar, there is a sidebar with 'Administration' selected, and a main content area with 'System > Administration > Web' selected. The 'Web' configuration page contains two panels: 'Configure Web' and 'SSL Certificate'. The 'Configure Web' panel has radio buttons for 'Enable' and 'Disable' for both HTTP and HTTPS, with 'Enable' selected for both. Below these are input fields for 'HTTP Port' (80) and 'HTTPS Port' (443), and a 'Web Refresh Period' of 10 seconds. The 'SSL Certificate' panel has a 'Certificate File (PEM format):' label, a 'Browse...' button, and a 'Submit' button at the bottom.

### 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.

The screenshot displays the MM ShutdownAgent web interface. At the top, the logo for MINUTE MAN POWER TECHNOLOGIES is visible on the left, and the title "MM ShutdownAgent" is centered. On the right, there are links for "Home" and "Logout". Below the header, a navigation bar includes "Monitor", "Device", and "System". The "System" tab is active, and the breadcrumb trail shows "System » Administration » Batch Configuration". The left sidebar contains a menu with "Information", "Login User", "Web", and "Batch Configuration" (which is selected). The main content area features a "System Configuration" section with a "Configuration File:" label and a "Download" button. Below this is a text input field with "Browse..." and "Upload" buttons. A "Description" section explains the batch configuration process, followed by five numbered steps: Step 1 (Download button), Step 2 (File format), Step 3 (Edit file), Step 4 (Upload button), and Step 5 (Wait for update). A "Submit" button is located at the bottom of the configuration area.

## 6. 2008 Server Core Setup for the ShutdownAgent

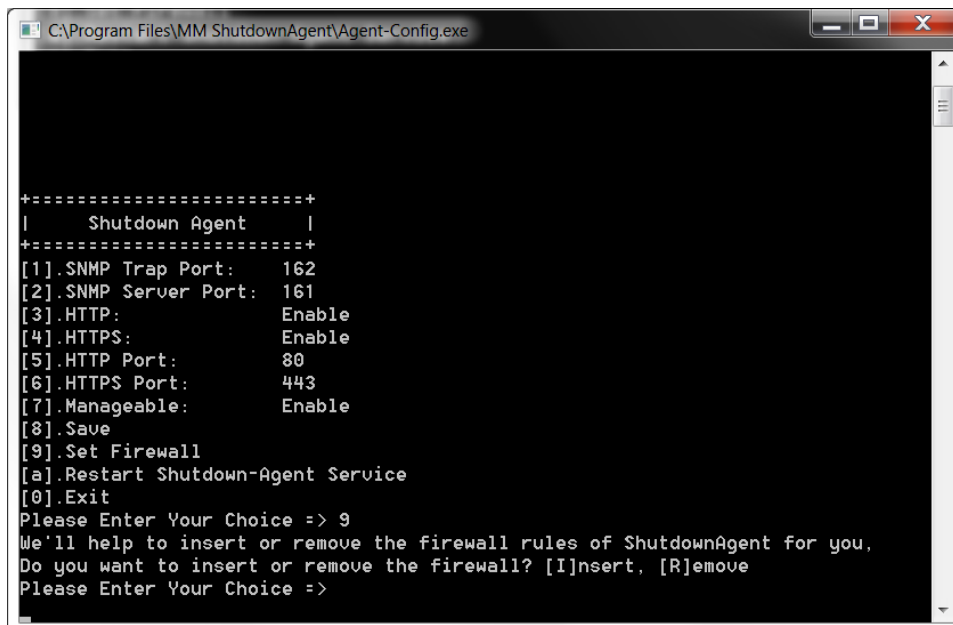
When installing the ShutdownAgent for the 2008 server core, it requires the following commands to transfer the file and add rules for firewall.

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.



```

C:\Program Files\MM ShutdownAgent\Agent-Config.exe

+-----+
|   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.

```

C:\Program Files\MM ShutdownAgent\Agent-Config.exe
+-----+
| 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]nset, [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.

The screenshot shows the configuration page for the MM ShutdownAgent. The interface includes a navigation menu on the left with options like 'Configure', 'Control', and 'Forward Trap'. The main content area is titled 'Device » Host » Configure' and is divided into several sections:

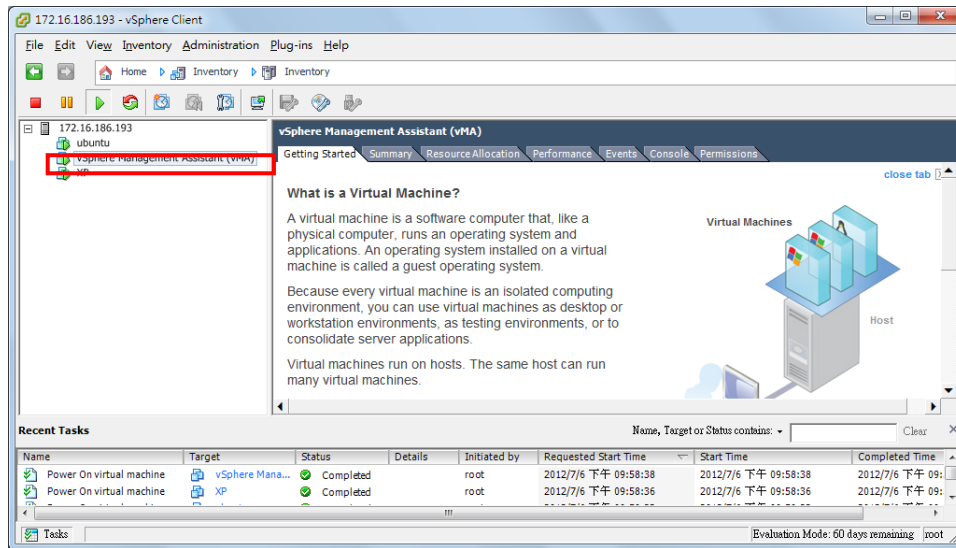
- Shutdown:** A table lists three shutdown events: 'Power Fail' (300s), 'Battery Low' (30s), and 'Smart Shutdown' (30s). Each event has an 'Enable' checkbox checked. A 'Submit' button is at the bottom.
- Reaction:** Contains two checked options: 'Notify Message' (with a 60s period) and 'Execute Command File' (with a file path and a 120s 'Run Before Shutdown' period). A 'Submit' button is at the bottom.
- Source IP:** Includes fields for 'Receive Trap Port' (162), 'Purpose' (radio buttons for 'For Redundant (Logical OR)' and 'For Parallel (Logical AND)'), 'Source Trap IP' (192.168.168.239), 'Community' (public), and 'SNMPv3 User'. A 'Submit' button is present.
- Manageable:** A checked checkbox 'Allow the ShutdownAgent to be managed by an authenticated manager.' with a 'Submit' button.

A table at the bottom right lists the configured Source IP entries:

IP Address	Community	SNMPv3 User
1 192.168.168.239	public	

## 8. VMWare ESXi5 Setup for the ShutdownAgent

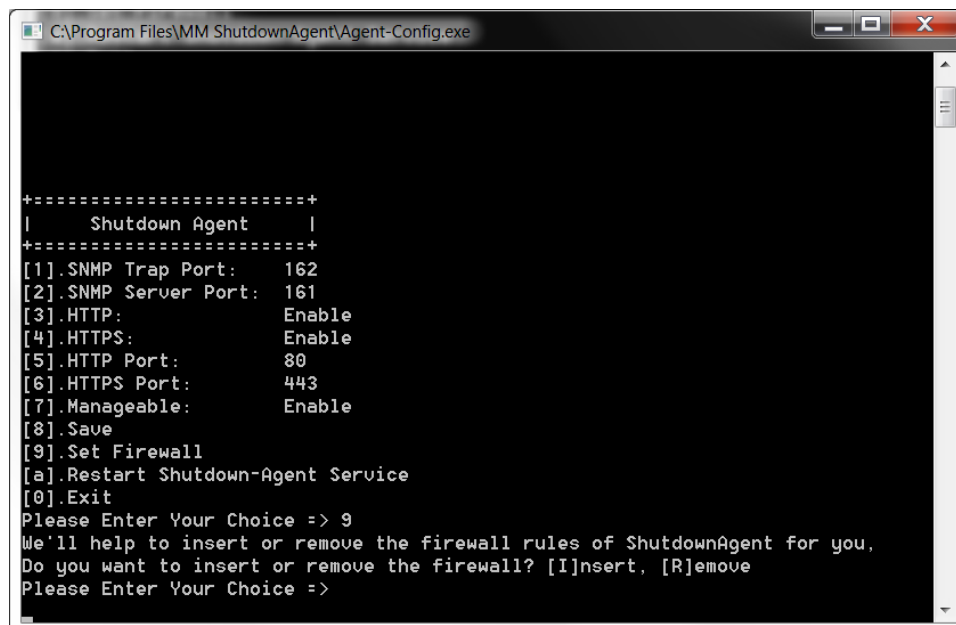
Before installing the ShutdownAgent for the ESXi5, you have to install the **vMA 5(vSphere Management Assistant 5)** and make sure the **VMWare tools** is installed on all of the guest OSes. Then transmit the ShutdownAgent setup file to the vMA server through SFTP by FileZilla FTP Client or another SFTP 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.



### 8.1 Configure the Firewall for vMA

Run the `/usr/local/upsagent/configure`

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



## 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 **/usr/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.

The screenshot displays the MM ShutdownAgent web interface. The top navigation bar includes 'Monitor', 'Device', and 'System' tabs. The 'Device' tab is active, showing 'Host' and 'SNMP' sub-tabs. The 'Configure' page is open, showing the following configuration sections:

- Shutdown:** Shutdown Type: Shutdown. A table lists events with checkboxes for enablement and OS Shutdown Delay in seconds.
 

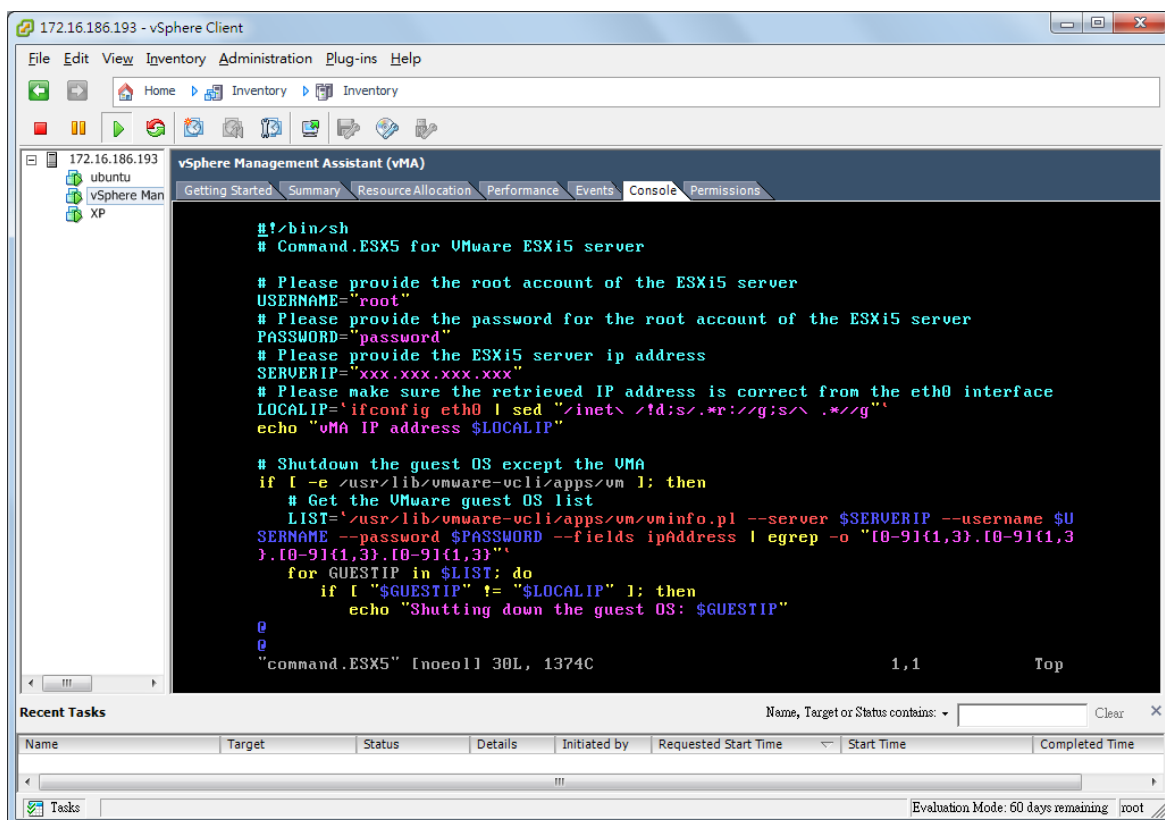
	Enable	Event	OS Shutdown Delay (in seconds)
1	<input checked="" type="checkbox"/>	Power Fail	300 second(s)
2	<input checked="" type="checkbox"/>	Battery Low	30 second(s)
3	<input checked="" type="checkbox"/>	Smart Shutdown	30 second(s)
- Reaction:**
  - Notify Message, Period: 60 second(s)
  - Execute Command File, File: /usr/local/upsagent/command/command.ESX5, 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: [empty].
- Manageable:**  Allow the ShutdownAgent to be managed by an authenticated manager.

Buttons for 'Submit', 'Add', 'Update', and 'Delete' are present throughout the interface.

## 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/.*://g;s/\ .*//g")
echo "vMA IP address $LOCALIP"

# Shutdown the guest OS except the vMA
if [ -e /usr/lib/vmware-uclicl/apps/vm ]; then
# Get the VMware guest OS list
LIST=$(/usr/lib/vmware-uclicl/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"
fi
done
fi
"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 the Citrix 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 `/usr/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.

The screenshot displays the MM ShutdownAgent web interface. The top navigation bar includes 'Monitor', 'Device', and 'System' tabs, with 'Device' selected. The system time is 'Thu 12/13/2012 PM 02:19:30'. The main content area is titled 'Device » Host » Configure' and contains several configuration panels:

- Shutdown:** A table with columns 'Enable', 'Event', and 'OS Shutdown Delay (in seconds)'. It lists three events: 'Power Fail' (300s), 'Battery Low' (30s), and 'Smart Shutdown' (30s). A 'Submit' button is at the bottom.
- Reaction:** Includes checkboxes for 'Notify Message' (period: 60s) and 'Execute Command File'. The command file path is '/usr/local/upsagent/command/command.Xen'. A 'Run Before Shutdown' field is set to 120s. A 'Submit' button is at the bottom.
- Source IP:** Includes 'Receive Trap Port' (162), 'Purpose' (radio buttons for 'For Redundant (Logical OR)' and 'For Parallel (Logical AND)'), 'Source Trap IP' (192.168.168.239), 'Community' (public), and 'SNMPv3 User'. A table below lists the configuration for IP Address, Community, and SNMPv3 User.
- Manageable:** Includes a checkbox 'Allow the ShutdownAgent to be managed by an authenticated manager' and a 'Submit' button.



## 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 **/usr/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.

The screenshot displays the MM ShutdownAgent web interface. The top navigation bar includes 'Monitor', 'Device', and 'System' tabs, with 'Device' selected. The 'Host' configuration page is active, showing various settings:

- Shutdown:** A table lists three events: Power Fail (300s), Battery Low (30s), and Smart Shutdown (30s). All are enabled.
- Reaction:** 'Notify Message' is checked with a 60s period. 'Execute Command File' is checked with the path `/usr/local/upsagent/command/command.KVM` and a 'Run Before Shutdown' of 120s.
- Source IP:** 'Receive Trap Port' is 162. 'Purpose' is set to 'For Redundant (Logical OR)'. 'Source Trap IP' is 192.168.168.239, and 'Community' is public.
- Manageable:** 'Allow the ShutdownAgent to be managed by an authenticated manager' is checked.

# 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.

The screenshot shows the 'SNMP-NV6 Web' interface. The left sidebar contains navigation options: User Manager, TCP/IP, Web, Console, FTP, Time Server, Syslog, Batch Configuration, and Upgrade. The main content area is titled 'System » Administration » TCP/IP'. It features two configuration panels: 'TCP/IP Settings for IPv4' and 'TCP/IP Settings for IPv6'. In the IPv4 settings, the 'IP Address' field is highlighted with a red box and contains the value '192.168.168.239'. The IPv6 settings show 'DHCP Client' set to 'Disable' and 'IP Address' as 'fe80::230:abff:fe2'. To the right, the 'System' panel shows 'Host Name: SNMP-NV6', 'System Contactor: Para', and 'System Location: CLT4R3'. Below this is a 'Link' section with 'Auto-Negotiation' checked and 'Speed' set to '100M'. A 'Submit' button is located at the bottom of the System panel.

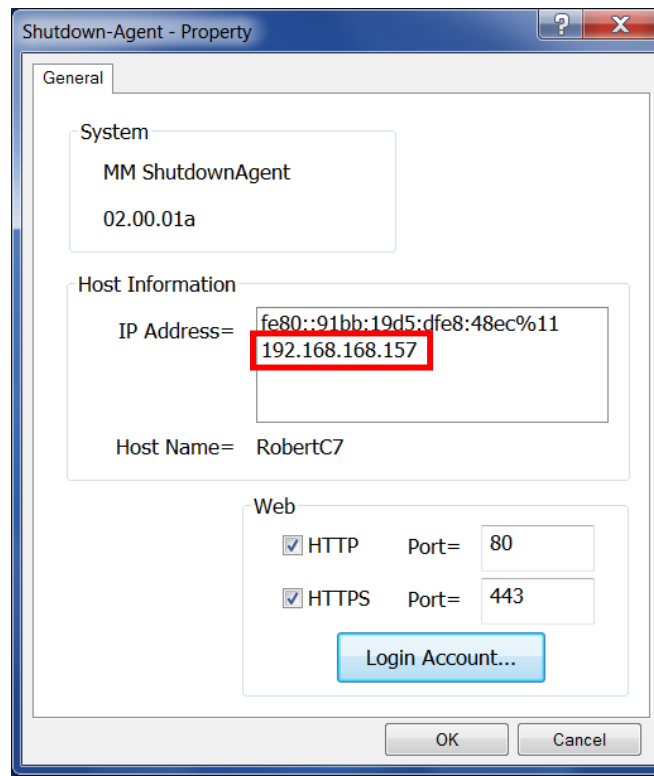
3. Login to the ShutdownAgent and add the SNMP-NV6 card's IP address and the trap port to receive the SNMP trap from the SNMP-NV6 card.

The screenshot shows the 'MM ShutdownAgent' interface. The left sidebar has 'Configure', 'Control', and 'Forward Trap' options. The main content area is titled 'Device » Host » Configure'. It contains several configuration panels: 'Shutdown' with a table of events (Power Fail, Battery Low, Smart Shutdown) and their OS Shutdown Delays; 'Reaction' with 'Notify Message' checked and a period of 60 seconds; 'Source IP' with 'Receive Trap Port' set to 162 and 'Source Trap IP' set to 192.168.168.239; and 'Manageable' with 'Allow the ShutdownAgent to be managed by an authenticated manager' checked. A table at the bottom lists the Source IP configuration with IP Address '192.168.168.239' and Community 'public'. A 'Submit' button is present at the bottom of the Manageable panel.

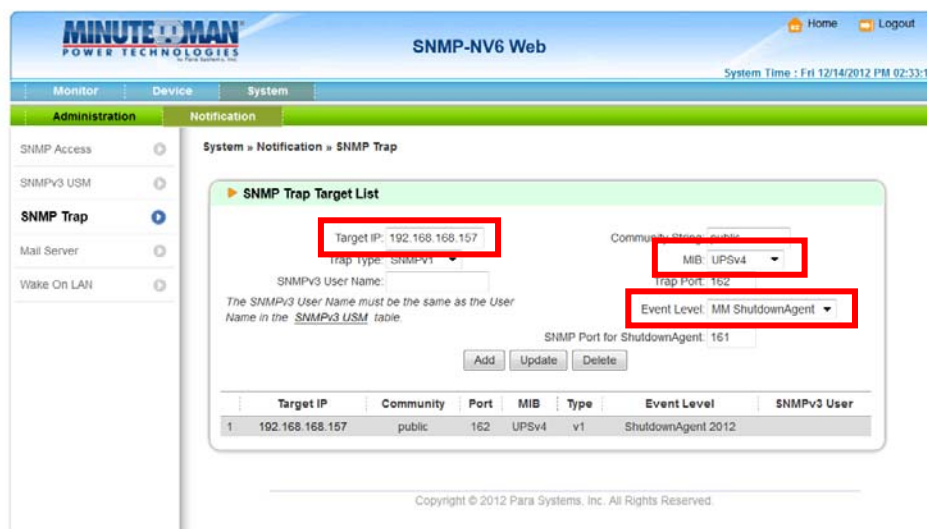
Enable	Event	OS Shutdown Delay (in seconds)
<input checked="" type="checkbox"/>	Power Fail	300 second(s)
<input checked="" type="checkbox"/>	Battery Low	30 second(s)
<input checked="" type="checkbox"/>	Smart Shutdown	30 second(s)

IP Address	Community	SNMPv3 User
1 192.168.168.239	public	

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



- 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.

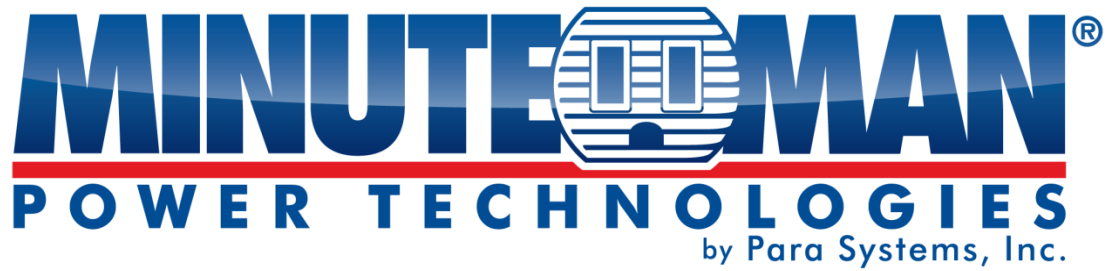


- If you enable the Manageable option in the ShutdownAgent then you can monitor the status of the ShutdownAgents from the SNMP-NV6 card (Monitor >> Information >> ShutdownAgent).



## 11.2 SNMP-NET Card

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



# MM ShutdownAgent

## Manuel d'utilisation

Pour obtenir les renseignements les plus à jour, veuillez consulter la traduction originale en anglais. Si vous avez des questions sur l'exactitude des spécifications traduites, des informations de garantie, des caractéristiques du produit, etc., veuillez contacter notre équipe de service à la clientèle.

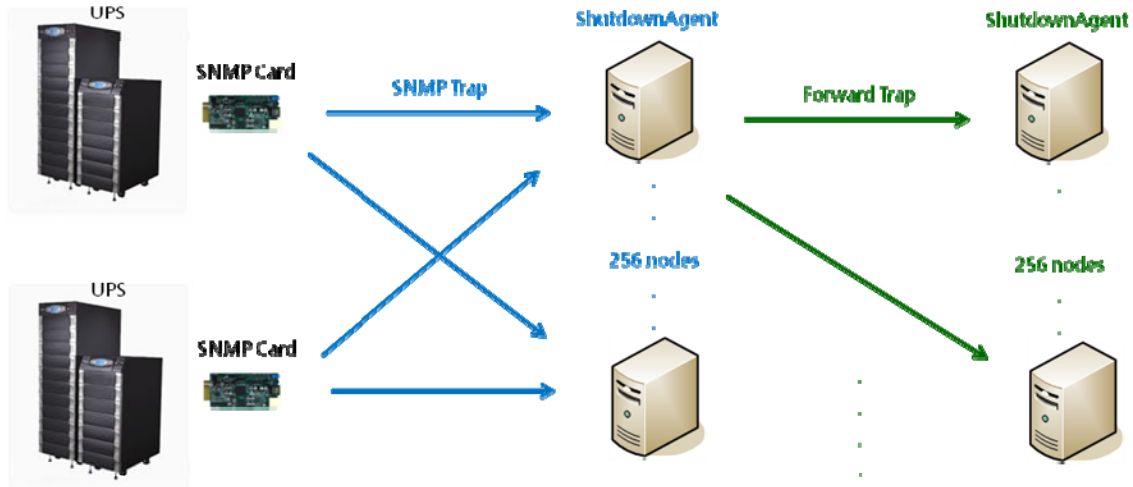
# Contenu

<b>1.Présentation générale.....</b>	<b>3</b>
1.1 Caractéristiques .....	3
1.2 Prise en charge du système d'exploitation.....	3
<b>2.Installation / Désinstallation .....</b>	<b>4</b>
2.1 Pour le système Windows .....	4
2.1.1 Processus d'installation .....	4
2.1.2 Processus de désinstallation.....	8
2.2 Pour le système Linux .....	8
2.2.1 Processus d'installation .....	8
2.2.2 Processus de désinstallation.....	9
<b>3.Configuration de la console .....</b>	<b>10</b>
3.1 Menu de la console .....	10
<b>4.Fonctionnement sous Windows.....</b>	<b>11</b>
4.1 Moniteur Web .....	11
4.2 Propriété.....	12
4.3 Afficher le compte à rebours .....	13
4.4 Annuler le compte à rebours .....	13
4.5 Arrêt du service .....	13
<b>5.Interface Web .....</b>	<b>14</b>
5.1 Exécuter un navigateur Web .....	14
5.2 Moniteur >> Informations >> Résumé.....	15
5.3 Moniteur >> Renseignements >> Journal des événements .....	16
5.4 Surveiller >> Informations >> Configurer le journal.....	17
5.5 Surveiller >> À propos >> Informations.....	17
5.6 Appareil >> Hôte >> Configurer .....	17
5.7 Appareil >> Hôte >> Contrôle .....	20
5.8 Appareil >> Hôte >> Interruption de transfert .....	20
5.9 Appareil >> SNMP >> Accès SNMP.....	21
5.10 Appareil >> SNMP >> SNMPv3 USM.....	21
5.11 Système >> Administration >> Informations.....	22
5.12 Système >> Administration >> Connexion utilisateur .....	22
5.13 Système >> Administration >> Web .....	23
5.14 Système >> Administration >> Configuration par lots .....	24
<b>6.2008 Configuration du serveur principal pour ShutdownAgent.....</b>	<b>25</b>
<b>7.Configuration de VMWare ESXi4 pour ShutdownAgent.....</b>	<b>26</b>
7.1 Configurer le pare-feu pour ESXi 4 .....	26
7.2 Installer VMware Tools pour le système d'exploitation invité .....	26
7.3 Configurer ShutdownAgent pour ESXi4 .....	26
<b>8.Configuration de VMWare ESXi5 pour ShutdownAgent.....</b>	<b>28</b>

8.1 Configurer le pare-feu pour vMA .....	28
8.2 Installer VMware Tools pour le système d'exploitation invité .....	29
8.3 Configurer ShutdownAgent pour ESXi5 .....	29
8.4 Modifier la commande Command.ESX5 .....	30
<b>9. Configuration de XenServer pour ShutdownAgent .....</b>	<b>31</b>
9.1 Installer le pilote PV pour le système d'exploitation invité .....	31
9.2 Configurer ShutdownAgent pour Xen .....	31
<b>10. Configuration KVM Linux pour ShutdownAgent .....</b>	<b>32</b>
10.1 Installer les outils libvirt pour KVM.....	32
10.2 Configurer ShutdownAgent pour KVM.....	32
<b>11. Utilisation de la carte SNMP .....</b>	<b>33</b>
11.1 Carte SNMP-NV6 .....	33
11.2 Carte SNMP-NET.....	35

# 1. Présentation

Le logiciel MM ShutdownAgent peut protéger le système d'exploitation en cas de panne de courant. À l'aide d'un navigateur Web, vous pouvez facilement obtenir les événements UPS actuels, la stratégie d'arrêt et les informations de compte à rebours.



## 1.1 Caractéristiques

1. Prend en charge les interruptions SNMPv1 et SNMPv3.
2. Prend en charge l'accès au serveur SNMPv1, SNMPv3 pour surveiller l'état de ShutdownAgent et configurer les paramètres d'arrêt.
3. Fournit une interface Web par HTTP et HTTPS.
4. Fournit une configuration par lots.
5. Peut transférer des interruptions SNMP vers 255 serveurs.
6. Prend en charge jusqu'à 32 sources de pièges pour les applications redondantes (OU logique) et parallèles (ET logique).
7. Fournit la configuration de la console pour les paramètres du système de base.
8. Prend en charge les programmes Windows 32/64 bits.

## 1.2 Support du système d'exploitation

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



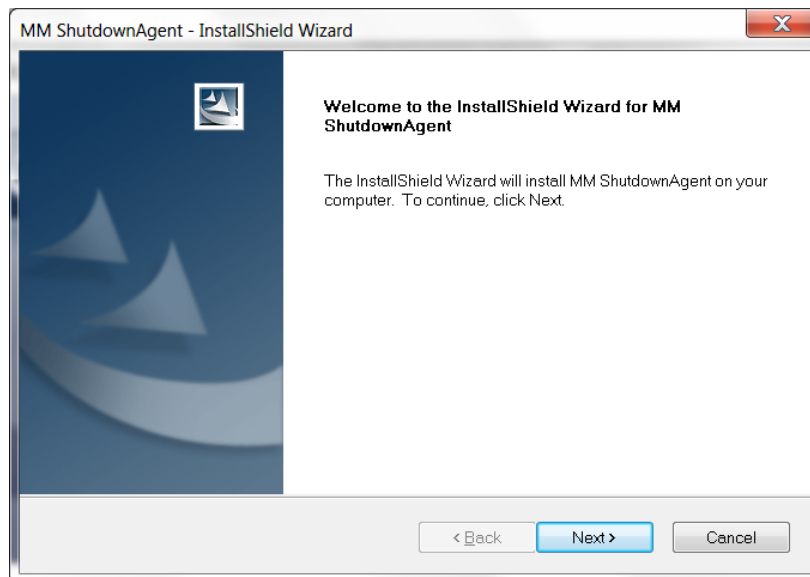
## 2. Installation / Désinstallation

### 2.1 Pour le système Windows

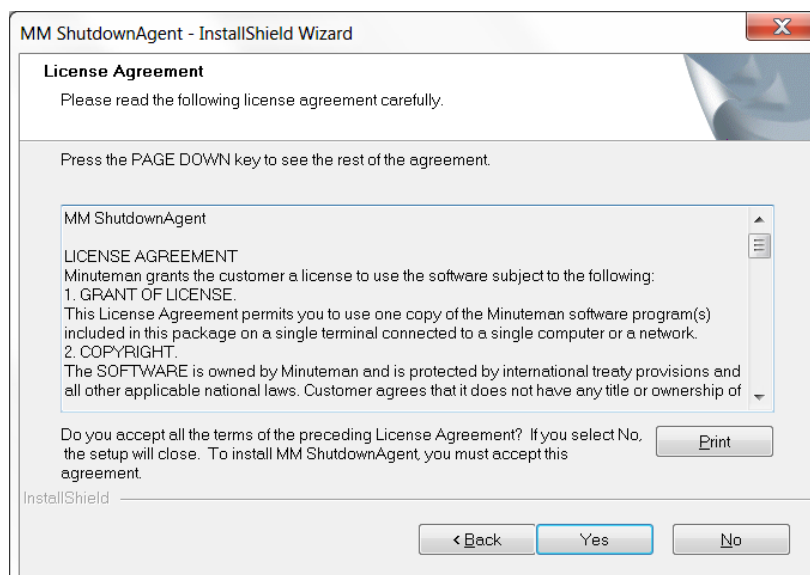
Il existe deux installateurs : MM-ShutdownAgent-Setup(win32).exe et MM-ShutdownAgent-Setup(x64).exe. L'un est pour le système d'exploitation Windows 32 bits et l'autre pour l'environnement Windows 64 bits.

#### 2.1.1 Processus d'installation

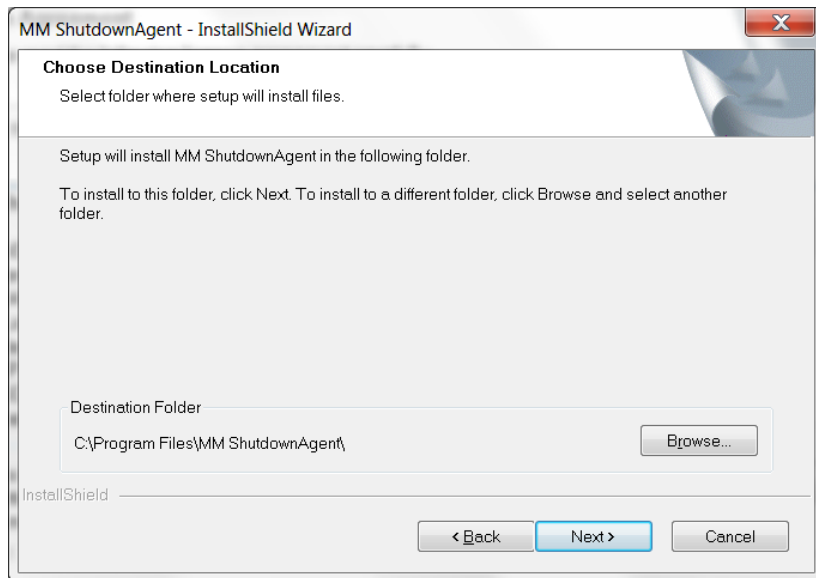
1. Exécutez MM-ShutdownAgent-Setup (xxx).exe pour exécuter le programme d'installation.
2. La page d'accueil s'affiche, appuyez sur le bouton « Suivant » pour poursuivre l'installation.



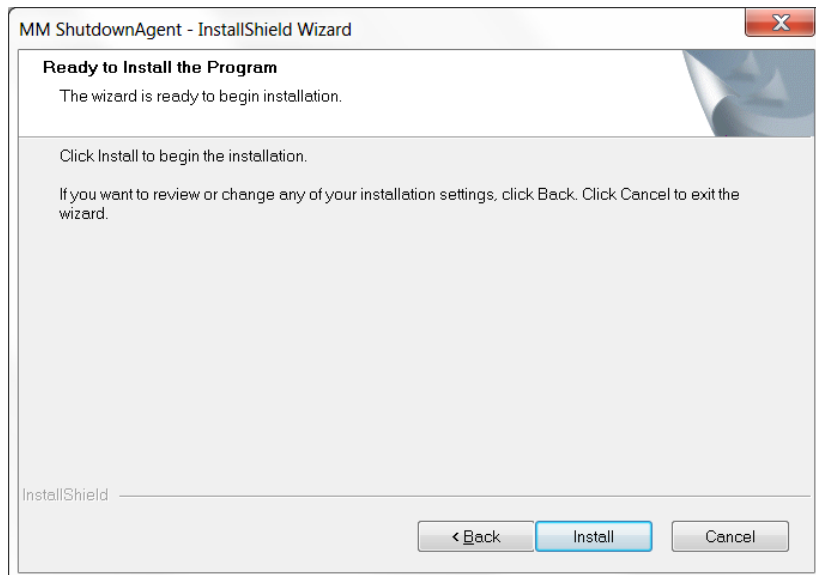
3. Appuyez sur le bouton « Oui » pour accepter le contrat de licence et poursuivre l'installation.



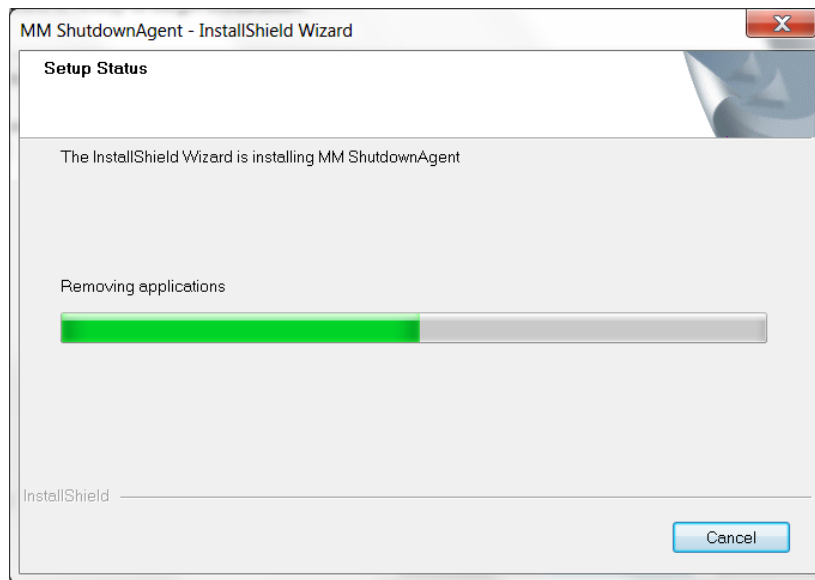
4. Sélectionnez un autre emplacement en utilisant le bouton Parcourir ou appuyez sur le bouton « Suivant » pour installer le logiciel à l'emplacement par défaut.



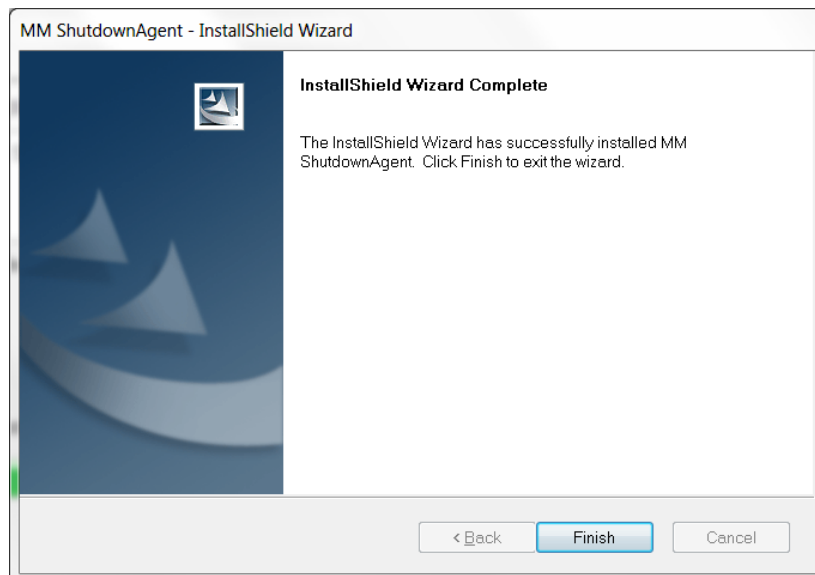
5. Appuyez sur le bouton « Installer » pour démarrer l'installation du logiciel à l'emplacement désigné.



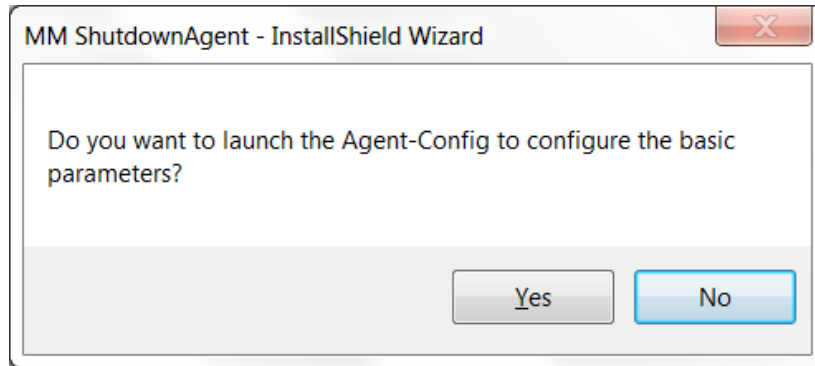
## 6. L'installation est en cours.



## 7. Une fois l'installation terminée, appuyez sur le bouton « Terminer » pour quitter le processus d'installation.



8. Une fois l'installation terminée, ShutdownAgent démarrera automatiquement le programme de service et ajoutera une icône pour indiquer son état dans la barre des tâches / menu Démarrer. Pendant ce temps, une boîte de dialogue apparaîtra pour vous demander si vous souhaitez lancer l'application Agent-Config pour configurer les paramètres de base. Appuyez sur le bouton Oui pour lancer l'Agent-Config à configurer en mode Shell (voir Chapitre 3). Ou appuyez sur le bouton Non pour terminer l'installation, puis ouvrez le menu Démarrer et recherchez le dossier MM ShutdownAgent pour utiliser la configuration de la console ou le moniteur Web pour configurer les paramètres du logiciel.



Le **Agent d'arrêt** le logiciel est composé de deux modules :

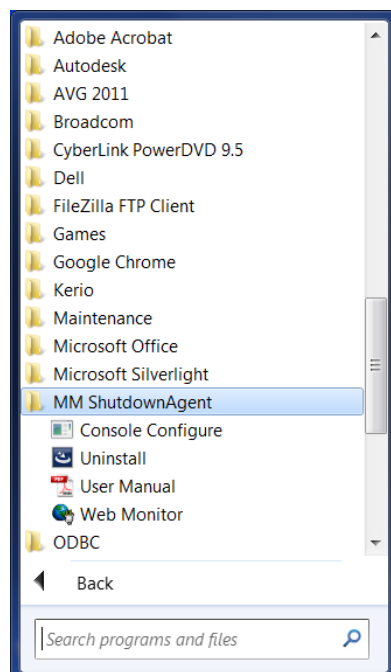
UN **Service** module (**Shutdown-Agent Service: Agent-Service.exe**), qui s'exécute en arrière-plan en tant que service et écoute l'interruption SNMP des adresses IP sources. UN **Statut** module (**Agent-Status.exe**), qui vous permet de contrôler et de configurer le logiciel par le biais de menus déroulants et de boîtes de dialogue. Il vous permet également de lancer le navigateur Web et de vous connecter automatiquement pour surveiller, configurer et contrôler le logiciel.

Une fois l'installation terminée, le programme d'installation créera une association MM ShutdownAgent avec les raccourcis suivants :

**Configuration de la console:** Lance l'Agent-Config.exe pour configurer les paramètres de base. **Désinstaller** : Supprime le MM ShutdownAgent. Les données de configuration seront toujours conservées dans le répertoire installé.

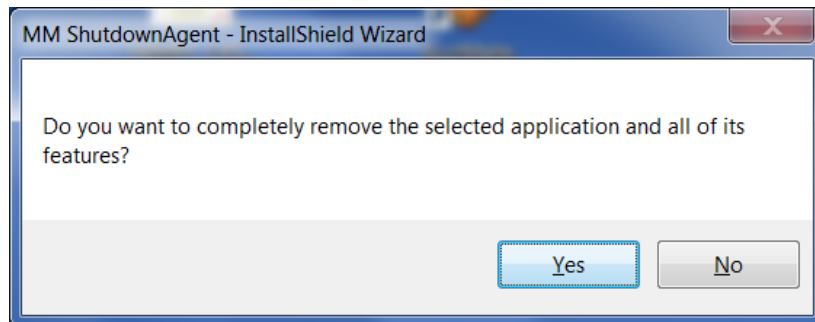
**Manuel d'utilisation** Le manuel d'utilisation est en format PDF.

**Moniteur Web:** L'interface utilisateur de MM ShutdownAgent utilisée pour surveiller et configurer le logiciel.

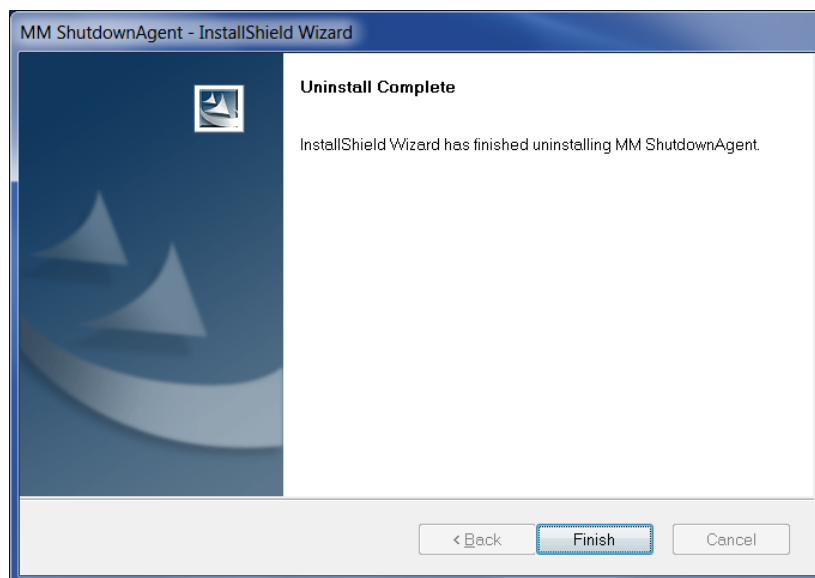


### 2.1.2 Processus de désinstallation

1. Sélectionnez Désinstaller dans le dossier du programme MM ShutdownAgent pour démarrer le processus de désinstallation.  
Vous pouvez également démarrer le processus de désinstallation de MM ShutdownAgent à partir de l'option Ajout/Suppression de programmes dans le Panneau de configuration.
2. Appuyez sur le bouton OK pour confirmer la suppression de toutes les applications ou sur le bouton Annuler pour annuler le processus de désinstallation.



3. Appuyez sur le bouton Terminer pour terminer le processus de désinstallation.



## 2.2 Pour le système Linux

### 2.2.1 Processus d'installation

1. Connectez-vous au système Linux et accédez au compte root : su  
root
2. Copiez le fichier MM-Shutdownagent-linux.tar.gz dans le répertoire /tmp :  
cp MM-Shutdownagent -linux.tar.gz /tmp
3. Changez votre répertoire de travail en /tmp :  
cd /tmp
4. décompressez le fichier MM-Shutdownagent  
-linux.tar.gz : gunzip MM-Shutdownagent -linux.tar.gz

5. extraire le fichier MM-Shutdownagent -linux.tar :

```
tar xvf MM-Shutdownagent -linux.tar
```

6. Exécutez le script d'installation :

```
./installer
```

```
+-----+ |
| MM ShutdownAgent 0.0.1 pour Linux |
| Copyright (c) 2012, Minuteman UPS. Tous |
| droits réservés. |
+-----+

Voulez-vous installer le MM ShutdownAgent? [y|n]
```

7. Appuyez sur « y » pour poursuivre le processus d'installation :

```
+-----+ |
| MM ShutdownAgent 0.0.1 pour Linux |
| Copyright (c) 2012 Minuteman UPS. Tous |
| droits réservés. |
+-----+

Le répertoire de destination est /usr/local/upsagent.

Copie de fichiers ..... Lien de
service d'installation.

agent d'arrestation          0 : désactivé 1 : désactivé 2 : désactivé 3 : activé      4 : désactivé 5 : activé      6 : désactivé

Démarrage de MM ShutdownAgent(upsagentd) ... terminé

Voulez-vous configurer le MM ShutdownAgent maintenant ? [y|n]
```

8. Maintenant, MM ShutdownAgent a été installé dans le répertoire suivant `/usr/local/upsagent/` et le programme de service démarre automatiquement.

Appuyez sur « y » pour lancer le programme `/usr/local/upsagent/configure` pour configurer les paramètres de base de MM ShutdownAgent ou appuyez sur « n » pour terminer le processus d'installation.

Consultez le chapitre 3 pour plus d'informations si vous voulez configurer les paramètres de base.

### 2.2.2 Processus de désinstallation

1. Connectez-vous au système Linux et accédez au compte root : `su root`

2. Modifiez votre répertoire de travail en `/usr/local/upsagent` :  
`cd /usr/local/upsagent`

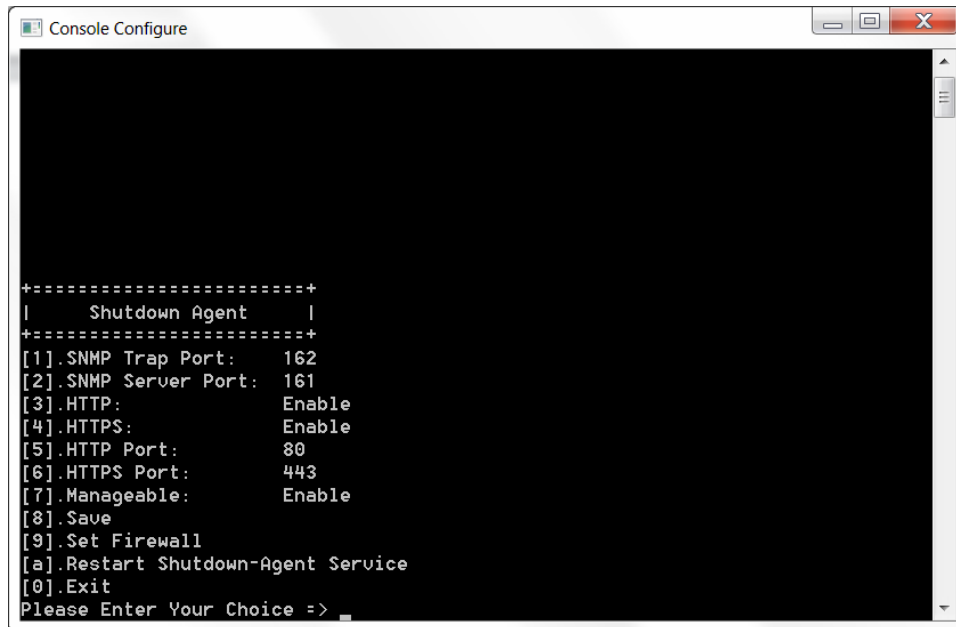
3. Exécutez le script de désinstallation pour supprimer MM ShutdownAgent :  
`./désinstaller`

4. Appuyez sur « y » pour démarrer le processus de désinstallation.

### 3. Configuration de la console

Le programme de configuration est conçu pour effectuer la configuration de base du MM ShutdownAgent en mode shell. Le logiciel peut être lancé à la fin du processus d'installation ou vous pouvez aller dans le répertoire installé pour le lancer manuellement.

Pour Windows, il se trouve dans « C:\Program Files\MM Shutdown Agent\Agent-Config.exe » Pour Linux, il se trouve dans « /usr/local/upsagent/configure »



```






Console 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 Menu console

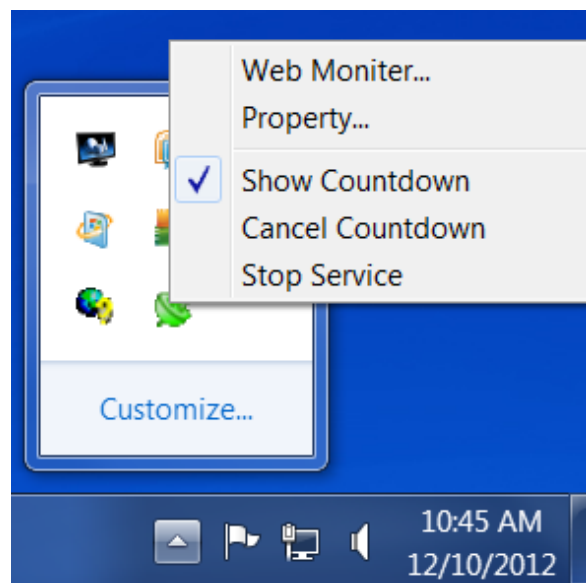
Non.	Fonction	Description	Défaut
1.	Port de trappe SNMP	Le port UDP pour écouter le trap SNMP	162
2.	Port du serveur SNMP	Le port UDP pour répondre aux commandes get/set	161
3.	HTTP	Activer ou désactiver le protocole HTTP	Autoriser
4.	HTTPS	Activer ou désactiver le protocole HTTPS	Autoriser
5.	Port HTTP	Le port TCP pour HTTP	80
6.	Port HTTPS	Le port TCP pour HTTPS	443
7.	Maniable	Autoriser un logiciel de gestion à gérer le ShutdownAgent	Autoriser
8.	Sauver	Sauvegardez les paramètres configurés dans agent.ini	
9.	Définir le pare-feu	Insérez ou supprimez la règle de pare-feu pour ShutdownAgent. Cette option est offerte pour tester rapidement la communication réseau. Les paramètres du pare-feu peuvent être récupérés après le redémarrage du système d'exploitation.	
un.	Redémarrage Service d'agent	Fermer Redémarrez le programme de service pour appliquer les modifications	
0.	Sortie	Quitter le programme de configuration	

## 4. Fonctionnement sous Windows

Après l'installation, ShutdownAgent place une icône dans la barre d'outils du bureau pour indiquer l'état de l'onduleur surveillé.

Icône	Description
	Normal
	Arrêt de service
	Onduleur en mode batterie
	Batterie UPS faible
	Onduleur en mode dérivation

Pour afficher le menu contextuel, déplacez le curseur sur l'icône ShutdownAgent et cliquez avec le bouton droit de la souris pour ouvrir le menu.



### 4.1 Moniteur Web

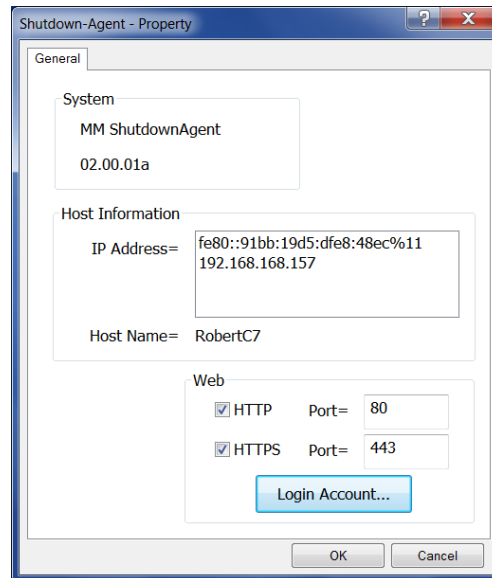
ShutdownAgent utilise une interface Web pour surveiller et configurer le logiciel. Sélectionnez le **Moniteur Web** menu pour lancer le navigateur Web par défaut. Si votre compte de connexion dans Windows appartient au groupe Administrateur local, ShutdownAgent se connectera automatiquement à son navigateur Web en tant qu'administrateur. Si vous connectez un navigateur Web à partir d'un ordinateur distant, vous devez entrer le nom d'utilisateur et le mot de passe. Le nom d'utilisateur par défaut est **administrateur** et le mot de passe par défaut est **mot de passe**.

Pour plus d'informations sur le fonctionnement du Web, consultez le chapitre 5.



## 4.2 Propriété

Le **Propriété** Le menu fournit un autre moyen de configurer les paramètres de base de ShutdownAgent. L'onglet Général affiche le numéro de version du logiciel, l'adresse IP du PC sur lequel le logiciel est installé, le nom de l'hôte et les ports.



### HTTP:

Pour activer/désactiver le protocole HTTP, attribuez un numéro différent au port pour modifier la connexion HTTP. Le port par défaut est 80. Si vous modifiez le port HTTP de 80, vous devez entrer l'URL comme suit : `http://192.168.1.100:8001`  
192.168.1.100 est l'adresse IP du PC sur lequel ShutdownAgent est installé et 8001 est le numéro de port que vous avez attribué.

**REMARQUE:** Vérifiez le paramètre du pare-feu Windows si la connexion HTTP est refusée.

### HTTPS:

Pour activer/désactiver le protocole HTTPS, attribuez un numéro différent au port pour modifier la connexion HTTPS. Le port par défaut est 443. Si vous avez modifié le port HTTPS de 443, vous devez saisir l'URL comme suit : `https://192.168.1.100:4430` 192.168.1.100 est l'adresse IP du PC sur lequel ShutdownAgent est installé et 4430 est le numéro de port que vous avez attribué.

**REMARQUE:** Vérifiez le paramètre du pare-feu Windows si la connexion HTTPS est refusée.

### Connexion au compte:

ShutdownAgent implémente 3 niveaux d'authentification pour la connexion Web comme suit :

#### Administrateur:

A le droit exclusif de modifier les paramètres de ShutdownAgent. **Gestionnaire**

#### de périphériques:

Il n'est pas permis de modifier les paramètres du système, mais il a la possibilité de configurer les paramètres de l'appareil.

#### Utilisateur en lecture seule:

L'utilisateur n'est autorisé qu'à observer les appareils connectés.

Voici la liste des comptes et des mots de passe par défaut. Notez qu'ils sont sensibles à la casse.

	<b>Account</b>	<b>Password</b>
Administrateur	admin	password
Gestionnaire de périphériques	device	password
Utilisateur en lecture seule	user	password

The screenshot shows a 'Web Login Account' dialog box with three sections for user configuration:

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

A 'Save' button is located at the bottom right of the dialog.

#### 4.3 Afficher le compte à rebours

Le compte à rebours affichera la fenêtre du compte à rebours lorsque ShutdownAgent démarrera le compte à rebours pour l'arrêt du système d'exploitation.



#### 4.4 Annuler le compte à rebours

Sélectionnez Annuler le compte à rebours pendant le compte à rebours pour arrêter le processus d'arrêt. Pour reprendre le processus d'arrêt, désélectionnez l'option Annuler le compte à rebours.

**REMARQUE:**Lors d'un nouvel événement d'arrêt, le compte à rebours sera affiché.

#### 4.5 Arrêt du service

Sélectionnez Arrêter le service pour arrêter le module de service ShutdownAgent. Pour redémarrer les services, désélectionnez l'élément Arrêter le service.

## 5. Interface Web

### 5.1 Exécuter un navigateur Web

Pour vous connecter à un navigateur Web à partir du même PC sur lequel ShutdownAgent est installé, sélectionnez Web Monitor dans le menu de la barre d'outils. ShutdownAgent ouvrira votre navigateur Web par défaut et si votre compte Windows appartient au groupe Administrateur local, ShutdownAgent se connectera automatiquement en tant qu'administrateur.

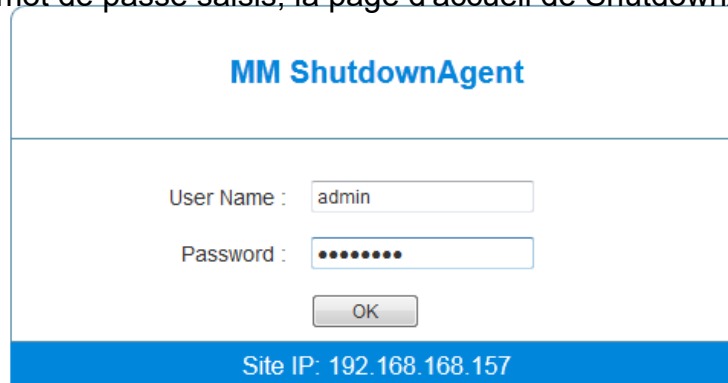
ShutdownAgent permet à un maximum de 16 utilisateurs de se connecter en même temps.

Vous pouvez également vous connecter avec un navigateur Web à partir d'un PC distant, comme suit :

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.

ShutdownAgent vous demandera alors votre nom d'utilisateur et votre mot de passe. Une fois le nom d'utilisateur et le mot de passe saisis, la page d'accueil de ShutdownAgent s'ouvre.



MM ShutdownAgent

User Name :

Password :

Site IP: 192.168.168.157

**REMARQUE:**ShutdownAgent déconnectera automatiquement l'utilisateur s'il n'y a pas de transmission de données pendant 30 minutes.

## 5.2 Moniteur >> Renseignements >> Résumé

Cette page contient des informations sur l'hôte, l'état d'arrêt, l'état IP source du piège SNMP et les 5 derniers événements.

**MINUTEMAN**  
POWER TECHNOLOGIES  
by Pare Systems, Inc.

**MM ShutdownAgent** Home Logout

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

Information About

**Summary** 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: 00:00

**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

Event Log...

### Hôte:

Énumérez le nom de l'hôte, le port UDP pour les interruptions SNMP et le système d'exploitation. **Fermer :**

Affiche le type d'arrêt (arrêt, mise hors tension, mise en veille prolongée) et le compte à rebours pour arrêter le système d'exploitation (lorsqu'il est activé). Le temps est affiché en secondes.

### Liste des adresses IP sources des interruptions SNMP :

ShutdownAgent est capable de recevoir des interruptions SNMP provenant de plusieurs hôtes sources, puis de répertorier l'événement comme OU logique pour une application redondante ou ET logique pour une application parallèle.

### Journal des 5 derniers événements :

Affiche les 5 derniers événements enregistrés. Pour voir la liste complète des événements enregistrés, cliquez sur le journal des événements dans le coin inférieur droit de cette page ou cliquez sur la page Journal des événements.

### 5.3 Surveiller >> Renseignements >> Journal des événements

Cette page Web énumère tous les événements qui ont été détectés par le logiciel. Les journaux existants sont écrasés lorsque le nombre maximal d'entrées (lignes) est atteint. Et le nombre maximal d'événements est de 10 000. Vous pouvez télécharger le journal des événements dans un format de fichier .csv.

#### Boutons de la page du journal :

Appuyez sur le bouton «<<» pour accéder à la page la plus récente et au bouton ">>» pour accéder à la page la plus ancienne.

Cliquez sur les boutons de numéro de page pour afficher le journal des événements par page.

#### Dates de début et de fin :

Vous pouvez filtrer le journal des événements par une plage de dates. Entrez les dates, puis appuyez sur le bouton Appliquer.

#### Télécharger tout :

Appuyez sur le **Télécharger tout** bouton pour exporter l'intégralité du journal des événements dans un format de fichier .csv.

The screenshot shows the MM Shutdown Agent web interface. The top navigation bar includes 'Monitor', 'Device', and 'System' tabs, with 'System' selected. The system time is displayed as 'Tue 12/11/2012 AM 11:17:26'. The left sidebar contains 'Summary', 'Event Log' (selected), and 'Log Configure'. The main content area displays the 'Event Log' for 'Page 1'.

The Event Log table has the following columns: IP Address, Date, Time, Level, and Event Log. The events listed are:

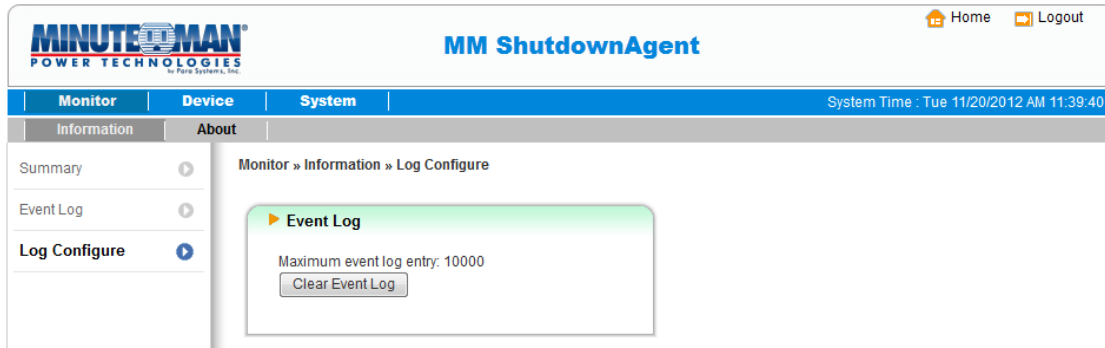
IP Address	Date	Time	Level	Event Log
192.168.168.239	12/11/2012	11:11:23	Information	Power restore
192.168.168.239	12/11/2012	11:11:03	Warning	Power fail
192.168.168.239	12/11/2012	11:09:20	Information	Power restore
192.168.168.239	12/11/2012	11:08:51	Warning	Power fail
	12/11/2012	11:02:03	System	Account 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 Surveiller >> Informations >> Configuration du journal

Cette page vous permet d'effacer le journal des événements.

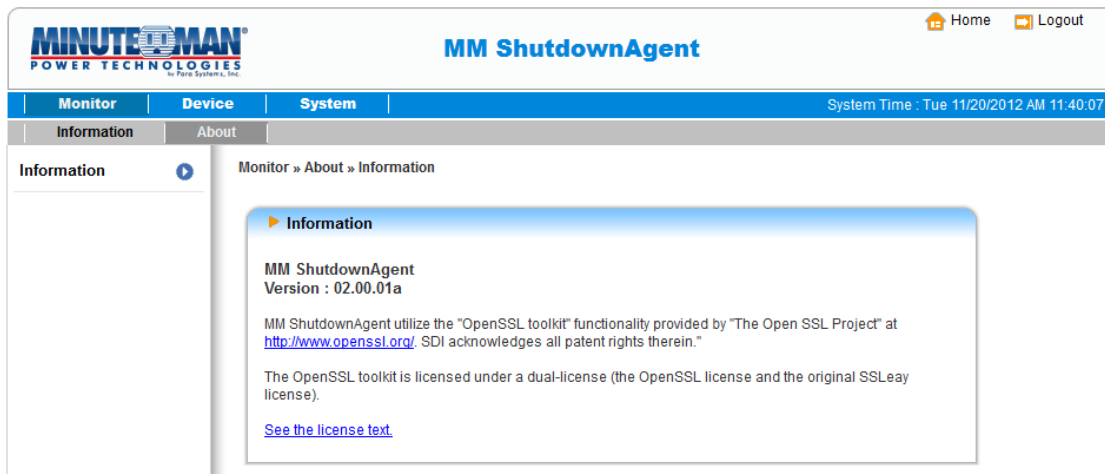
Effacer le journal des événements :

Cliquez sur ce bouton pour effacer le journal des événements.



## 5.5 Moniteur >> À propos >> Renseignements

Cette page affiche le numéro de version du logiciel et des renseignements importants sur la boîte à outils SSL utilisée par ce logiciel.



## 5.6 Appareil >> Hôte >> Configurer

Cette page permet de configurer les fonctions suivantes : Arrêt, Réaction, IP source et Gérable.

### Fermer :

Choisissez le bon **Type d'arrêt** pour arrêter le système d'exploitation. Il existe trois sélections pour le type d'arrêt : **Fermer**, **Éteindre** et **Hiberner**. La valeur par défaut est Arrêt.

Définissez le délai d'arrêt pour l'événement d'alimentation activé. Si l'événement d'alimentation se rétablit pendant le compte à rebours, l'action d'arrêt sera interrompue.

The screenshot shows the MM ShutdownAgent web interface. The top navigation bar includes 'Monitor', 'Device', and 'System' tabs, with 'Device' selected. The system time is 'Tue 11/20/2012 AM 11:42:05'. The main content area is titled 'Device » Host » Configure' and contains several configuration panels:

- Shutdown:** A table with columns 'Enable', 'Event', and 'OS Shutdown Delay (in seconds)'. It lists three events: 'Power Fail' (300s), 'Battery Low' (30s), and 'Smart Shutdown' (30s). A 'Submit' button is at the bottom.
- Reaction:** Includes a checked 'Notify Message' checkbox with a 'Period: 60 second(s)' field, and an unchecked 'Execute Command File' checkbox with a 'File:' input field and a 'Run Before Shutdown: 120 second(s)' field. A 'Submit' button is at the bottom.
- Source IP:** Includes a 'Receive Trap Port: 162' field, a 'Purpose:' section with radio buttons for 'For Redundant (Logical OR)' (selected) and 'For Parallel (Logical AND)', and a 'Submit' button. Below are fields for 'Source Trap IP: 0.0.0.0', 'Community: public', and 'SNMPv3 User:'. A table below lists 'IP Address', 'Community', and 'SNMPv3 User' with one entry: '1', '0.0.0.0', 'public'.
- Manageable:** Includes a checked checkbox 'Allow the ShutdownAgent to be managed by an authenticated manager.' and a 'Submit' button. A note below explains that the authenticated manager can be a SNMP card or centralized management software.

### Réaction:

Activer le **Message de notification** pour recevoir des messages contextuels une fois que ShutdownAgent reçoit une interruption SNMP. Attribuez la période de temps pour signaler le message périodiquement.

Activer le **Exécuter le fichier de commandes** pour exécuter un fichier externe attribué avant l'arrêt.

Définissez une heure pour le **Exécuter avant l'arrêt** pour informer ShutdownAgent quand lancer le fichier exécutable attribué.

### Source IP :

Attribuer le **Port de réception de piège** pour ouvrir un port UDP spécifique pour recevoir des interruptions SNMP. Sélectionnez ensuite le mode redondant (OU logique) ou parallèle (ET logique) pour l'application.

**Redondant (OU logique) :** Résume l'événement d'alimentation reçu par OU logique pour toutes les adresses IP sources afin de déterminer si l'événement d'alimentation s'est produit ou non. Si l'événement d'alimentation s'est produit dans l'une des adresses IP sources, l'événement d'alimentation est tenable et ShutdownAgent commence le compte à rebours en conséquence. Ce n'est que lorsque l'événement d'alimentation récupère toutes les adresses IP sources que ShutdownAgent s'arrête et annule le processus d'arrêt.

**Parallèle (ET logique) :** Résume l'événement d'alimentation reçu par ET logique pour toutes les adresses IP sources afin de déterminer si l'événement d'alimentation s'est produit ou non. Si l'événement d'alimentation s'est produit dans toutes les adresses IP sources, l'événement d'alimentation est tenable et ShutdownAgent commence le compte à rebours en conséquence. Une fois que l'événement d'alimentation est récupéré à partir de l'une des adresses IP sources, ShutdownAgent s'arrête et annule le processus d'arrêt.

**Adresse IP source :** Attribuer l'adresse IP source. ShutdownAgent analysera le piège SNMP uniquement lorsque le paquet sera reçu à partir des adresses IP attribuées. **Communauté:** Si une valeur de chaîne de communauté est attribuée, seul le piège reçu avec la même chaîne de communauté sera accepté. S'il n'y a pas de chaîne de communauté attribuée, ShutdownAgent acceptera n'importe laquelle des chaînes de communauté reçues.

**Utilisateur SNMPv3 :** Ce champ est utilisé pour les paquets SNMPv3. Si un utilisateur SNMPv3 est attribué, seul le piège reçu avec le même utilisateur défini dans la table USM SNMPv3 sera accepté. Si aucun utilisateur SNMPv3 n'est attribué, ShutdownAgent n'acceptera pas les utilisateurs assignés dans la table USM SNMPv3.

### Maniable :

Sélectionnez le **Autoriser la gestion de ShutdownAgent par un gestionnaire authentifié** option permettant à ShutdownAgent de répondre à la requête de n'importe quel gestionnaire authentifié. Le gestionnaire authentifié peut être une carte SNMP ou un logiciel de gestion centralisée. Après avoir recueilli les informations de ShutdownAgent, le gestionnaire authentifié peut fournir une liste complète de tous les ShutdownAgents.

Le gestionnaire authentifié communique avec ShutdownAgent via SNMPv3 avec le premier compte par défaut de la liste USM SNMPv3. Si cette option est activée, le compte du gestionnaire passe à « Lecture/Écriture », sinon l'autorisation est « Désactiver ». Le paramètre par défaut pour le **Autoriser la gestion de ShutdownAgent par un gestionnaire authentifié** est activé.



## 5.7 Appareil >> Hôte >> Contrôle

### Contrôler:

Appuyez sur le bouton Annuler le compte à rebours pendant le processus de compte à rebours pour arrêter l'arrêt.

Appuyez de nouveau sur le bouton pour reprendre le processus d'arrêt.

### Piège de simulation directe :

Appuyez sur le bouton Panne de courant pour envoyer l'interruption SNMP de panne de courant simulée aux adresses IP cibles de transfert attribuées.

Appuyez sur le bouton Restauration de l'alimentation pour envoyer l'interruption SNMP de restauration de l'alimentation simulée aux adresses IP cibles de transfert attribuées.

The screenshot shows the MM Shutdown Agent web interface. The top navigation bar includes the logo for MINUTE MAN POWER TECHNOLOGIES, the title MM ShutdownAgent, and links for Home and Logout. Below the navigation bar, there are tabs for Monitor, Device, and System, with the System Time displayed as Tue 11/20/2012 AM 11:42:57. The main content area is divided into Host and SNMP sections. The Host section has a sidebar with options: Configure, Control (selected), and Forward Trap. The main area shows the 'Device » Host » Control' page with two main panels: 'Control' and 'Forward Simulation Trap'. The 'Control' panel contains buttons for 'Cancel Countdown' and 'Pause Broadcast', with a note: 'Note: Selecting Pause Broadcast will stop the Broadcast messages until the next event occurs.' The 'Forward Simulation Trap' panel contains buttons for 'Power Fall' and 'Power Restore', with a note: '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 Appareil >> Hôte >> Interruption de transfert

Le Forward Trap est utilisé pour transférer les trappes SNMP reçues vers les adresses IP ciblées pour effectuer l'arrêt.

The screenshot shows the MM Shutdown Agent web interface. The top navigation bar includes the logo for MINUTE MAN POWER TECHNOLOGIES, the title MM ShutdownAgent, and links for Home and Logout. Below the navigation bar, there are tabs for Monitor, Device, and System, with the System Time displayed as Tue 11/20/2012 AM 11:43:45. The main content area is divided into Host and SNMP sections. The Host section has a sidebar with options: Configure, Control, and Forward Trap (selected). The main area shows the 'Device » Host » Forward Trap' page with a 'Target IP List' section. This section includes input fields for 'Target IP' (192.168.168.239) and 'UDP Port' (162, Default: 162), and buttons for 'Add', 'Update', and 'Delete'. Below the input fields is a table with the following data:

	Target IP	UDP Port
1	192.168.168.239	162

## 5.9 Appareil >> SNMP >> Accès SNMP

ShutdownAgent prend en charge le protocole SNMP et SNMP NMS (Network Management System), qui sont couramment utilisés pour surveiller les périphériques réseau afin de détecter les conditions nécessitant une attention administrative. Pour empêcher tout accès non autorisé, vous pouvez spécifier les adresses IP NMS, leurs chaînes communautaires et leurs niveaux d'accès. Le nombre maximal d'entrées IP est de 255.

The screenshot shows the 'SNMPv1 Access' configuration page in the MM ShutdownAgent interface. The page title is 'Device » SNMP » SNMPv1 Access'. The configuration form includes fields for 'SNMP Port' (161), 'Download MIB' (ShutdownAgent), 'Access IP' (0.0.0.0), 'Community' (public), and 'Permission' (Read Only). Below the form is a table listing the configured access entries.

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

## 5.10 Appareil >> SNMP >> SNMPv3 USM

SNMPv3 offre des fonctionnalités telles que le cryptage des paquets et l'authentification pour améliorer la sécurité. Le SNMPv3 USM (User Session Management) vous permet d'attribuer 32 noms d'utilisateur. Vous pouvez également définir leurs niveaux de sécurité respectifs, leurs mots de passe d'authentification, leurs mots de passe de confidentialité et leurs autorisations. Le premier compte ne peut pas être supprimé, pour le désactiver, allez à la page Web Appareil >> Hôte >> Configurer, puis décochez l'option gérable.

The screenshot shows the 'SNMPv3 USM' configuration page in the MM ShutdownAgent interface. The page title is 'Device » SNMP » SNMPv3 USM'. The configuration form includes fields for 'Context Name' (cn1027), 'Auth Protocol' (MD5), 'Priv Protocol' (CBC-DES), 'User Name' (manager), 'Auth Password', 'Priv Password', and 'Permission' (Read/Write). Below the form is a table listing the configured user sessions.

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

## 5.11 Système >> Administration >> Renseignements

Les renseignements système peuvent être configurés ici.

MINUTE MAN POWER TECHNOLOGIES

MM ShutdownAgent

Home Logout

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

Administration

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

Submit

## 5.12 Système >> Administration >> Connexion de l'utilisateur

L'authentification de connexion à l'interface Web peut être gérée en attribuant trois niveaux différents au compte et au mot de passe des utilisateurs.

Les autorisations d'accès pour les types de compte sont énumérées comme suit :

**Administrateur** :Autorisé à modifier tous les paramètres.

**Gestionnaire de périphériques** :Autorisé à modifier les paramètres liés à l'appareil.

**Utilisateur en lecture seule** :Autorisé à lire uniquement l'état de ShutdownAgent.

MINUTE MAN POWER TECHNOLOGIES

MM ShutdownAgent

Home Logout

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

Administration

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	.....

Submit

## 5.13 Système >> Administration >> Web

Ce menu permet à l'administrateur d'activer ou de désactiver les protocoles de communication HTTP/HTTPS disponibles dans ShutdownAgent.

The screenshot shows the MM ShutdownAgent web interface. The top navigation bar includes 'Monitor', 'Device', and 'System' tabs, with 'System' selected. The system time is 'Tue 11/20/2012 AM 11:48:42'. The left sidebar shows 'Administration' with sub-items: 'Information', 'Login User', 'Web' (selected), and 'Batch Configuration'. The main content area is titled 'System » Administration » Web' and contains two panels:

- Configure Web:**
  - HTTP:  Enable  Disable
  - HTTPS:  Enable  Disable
  - HTTP Port:
  - HTTPS Port:
  - Web Refresh Period:  Seconds
- SSL Certificate:**
  - Certificate File (PEM format):
  - Update the certificated file which is generated by openssl for new SSL connections.
  -

### HTTP :

Activation ou désactivation de la connexion HTTP avec ShutdownAgent.

### HTTPS :

Activation ou désactivation de la connexion HTTPS avec ShutdownAgent.

### Port HTTP :

L'utilisateur peut configurer le protocole HTTP pour utiliser un numéro de port autre que le port HTTP standard (80).

### Port HTTPS :

L'utilisateur peut configurer le protocole HTTPS pour utiliser un numéro de port autre que le port HTTPS standard (443).

### Période de rafraîchissement du site Web :

L'intervalle de temps d'actualisation de la page Web peut être configuré. La plage est de 1 à 9999 secondes.

### Certificat SSL :

Pour assurer la sécurité entre le ShutdownAgent et le poste de travail connecté, le certificat SSL peut être utilisé pour crypter et sécuriser l'intégrité des données transmises. **Fichier de certificat** : Cela vous permet de remplacer votre propre fichier de certificat SSL. ShutdownAgent prend en charge le format PEM généré par OpenSSL. Cliquez **Choisir le fichier** pour télécharger le fichier de certificat.

## 5.14 Système >> Administration >> Configuration par lots

ShutdownAgent fournit une configuration par lots pour permettre une configuration rapide et sans effort sur plusieurs hôtes ShutdownAgent. Vous pouvez dupliquer les paramètres en téléchargeant le fichier de configuration à partir du ShutdownAgent que vous avez configuré avec succès et en téléchargeant les fichiers de configuration sur plusieurs ShutdownAgents. Suivez simplement la procédure étape par étape.

### Télécharger:

Téléchargez le fichier agent.ini pour stocker ou modifier le fichier de configuration.

### Télécharger :

Téléchargez le fichier de configuration sur plusieurs ShutdownAgents.

The screenshot displays the MM ShutdownAgent web interface. At the top, there is a navigation bar with the logo for MINUTE MAN POWER TECHNOLOGIES and the title MM ShutdownAgent. Below this is a secondary navigation bar with tabs for Monitor, Device, and System. The main content area is titled 'System » Administration » Batch Configuration'. On the left, there is a sidebar menu with options: Information, Login User, Web, and Batch Configuration (which is currently selected). The main content area contains a 'System Configuration' section with a 'Configuration File:' label and a 'Download' button. Below this is a text input field with 'Browse...' and 'Upload' buttons. A 'Description' section explains that the batch configuration is used to configure all system parameters at once. It lists five steps: Step 1: Press the Download button to download the configure.ini file. Step 2: Follow the file format, including [Section] and [End] sections. Step 3: Edit the configure.ini file with text edit software. Step 4: Select the modified file and press the Upload button. Step 5: Wait for about 10 seconds for the system to update. A 'Submit' button is located at the bottom of the configuration area.

## 6. 2008 Configuration du serveur principal pour ShutdownAgent

Lors de l'installation de ShutdownAgent pour le serveur Core 2008, les commandes suivantes sont nécessaires pour transférer le fichier et ajouter des règles pour le pare-feu.

### 1. Désactiver le pare-feu :

```
netsh advfirewall a désactivé l'état de tous les profils
```

### 2. Activez le pare-feu :

```
netsh advfirewall définit l'état de tous les profils sur
```

### 3. Ajoutez un répertoire partagé à distance :

```
net use e: \\<adresse IP>\e
```

### 4. Ouvrez le piège SNMP UDP 162

```
netsh advfirewall pare-feu ajouter une règle nom="SNMPTrap" protocole=UDP dir=in localport=162 action = autoriser
```

### 5. Ouvrez le serveur SNMP UDP 161

```
netsh advfirewall pare-feu ajouter une règle nom="SNMPServer" protocole=UDP dir=in localport=161 action = autoriser
```

### 6. Ouvrez le HTTP TCP 80

```
netsh advfirewall pare-feu ajouter une règle nom = "HTTP" protocole = TCP dir = dans localport = 80 action = autoriser
```

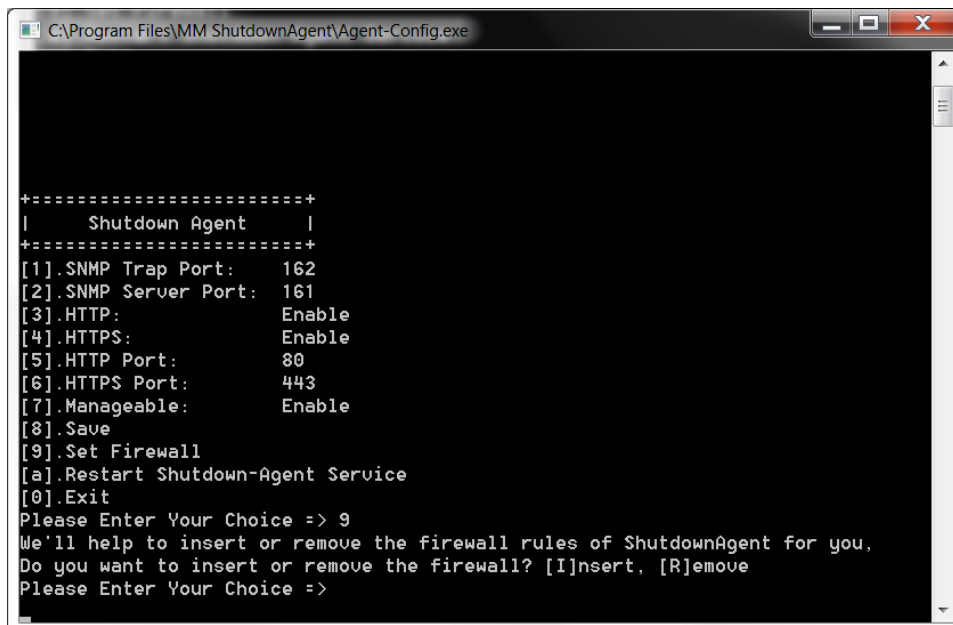
### 7. Ouvrez le HTTPS TCP 443

```
netsh advfirewall pare-feu ajouter une règle nom = "HTTPS" protocole = TCP dir = dans localport = 443 action = autoriser
```

Tout d'abord, placez le fichier d'installation Déplacer-Agent-2012-Setup(x64).exe dans le répertoire du serveur 2008. S'il n'y a pas de CD-ROM, vous pouvez définir la commande « Désactiver le pare-feu », la commande « Ajouter un répertoire partagé à distance » puis copier le fichier de votre PC vers le serveur 2008. N'oubliez pas de définir la commande « Activer le pare-feu » une fois terminé.

Deuxièmement, suivez le chapitre 2 pour installer ShutdownAgent sur le serveur 2008. La dernière étape consiste à utiliser les commandes open HTTP/HTTPS, SNMP Trap/Server port pour ouvrir les ports nécessaires. Vous pouvez facilement exécuter Agent-Config.exe pour configurer les paramètres réseau de base pour les protocoles réseau Web et SNMP après l'installation.

Sélectionnez [9] pour configurer le pare-feu pour ShutdownAgent.



```
C:\Program Files\MM ShutdownAgent\Agent-Config.exe

+*****+
|   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 =>
```

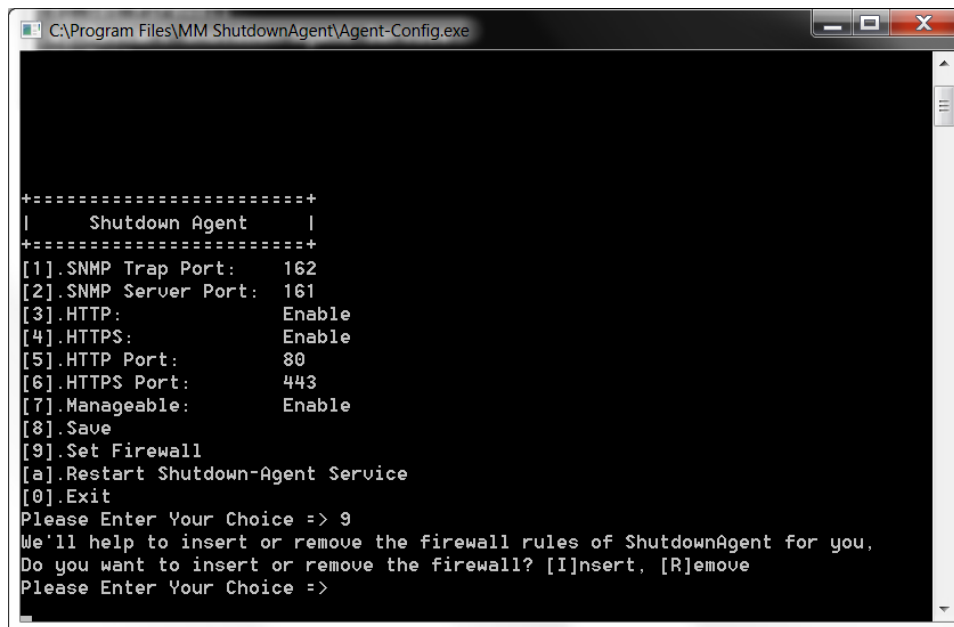
## 7. Configuration de VMWare ESXi4 pour ShutdownAgent

Avant d'installer ShutdownAgent sur le serveur ESXi4, transmettez le fichier d'installation de ShutdownAgent au serveur ESX via SFTP via le client FTP FileZilla ou un autre client SFTP, puis connectez-vous au serveur ESX via la console locale ou via votre client SSH (tel que Putty). Suivez la section 2.2 pour l'installation/désinstallation de Linux. Voir le chapitre 3 pour la configuration de la console.

### 7.1 Configurer le pare-feu pour ESXi 4

Exécutez `/usr/local/upsagent/configure`

Sélectionnez [9] pour configurer le pare-feu pour ShutdownAgent.



```

C:\Program Files\MM ShutdownAgent\Agent-Config.exe
+-----+
|   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 Installer VMware Tools pour le système d'exploitation invité

Pour arrêter le système d'exploitation invité du serveur ESXi, installez les outils VMware sur tous les systèmes d'exploitation invités pour effectuer l'arrêt correctement.

Pour le système d'exploitation Windows :

**Sélectionnez le menu suivant Invité - Installer/Mettre à niveau VMware Tools**

### 7.3 Configurer DélimitationAgent pour ESXi4

Entrez le temps estimé nécessaire pour que tous les systèmes d'exploitation invités qui fonctionnent sur le serveur ESXi4 s'arrêtent correctement.

1. Connectez-vous à l'interface Web de ShutdownAgent. Le niveau du compte doit être égal ou supérieur à celui du gestionnaire de périphériques.
2. Accédez à la page Web Appareil - Hôte - Configurer et entrez le temps estimé dans le champ **Exécuter avant l'arrêt** domaine de la **Réaction** groupe.
3. Entrez `/utilisateur/local/upsagent/commande/commande.ESX4` fichier de script pour ESXi 4 pour arrêter les systèmes d'exploitation invités. Cochez ensuite la case Exécuter le fichier de commande pour activer l'arrêt des systèmes d'exploitation invités.

4.Appuyez sur le**Soumettre** bouton pour mettre à jour vos modifications.

The screenshot shows the configuration page for the MM ShutdownAgent. The interface includes a navigation menu on the left with options like 'Configure', 'Control', and 'Forward Trap'. The main content area is titled 'Device » Host » Configure' and is divided into several sections:

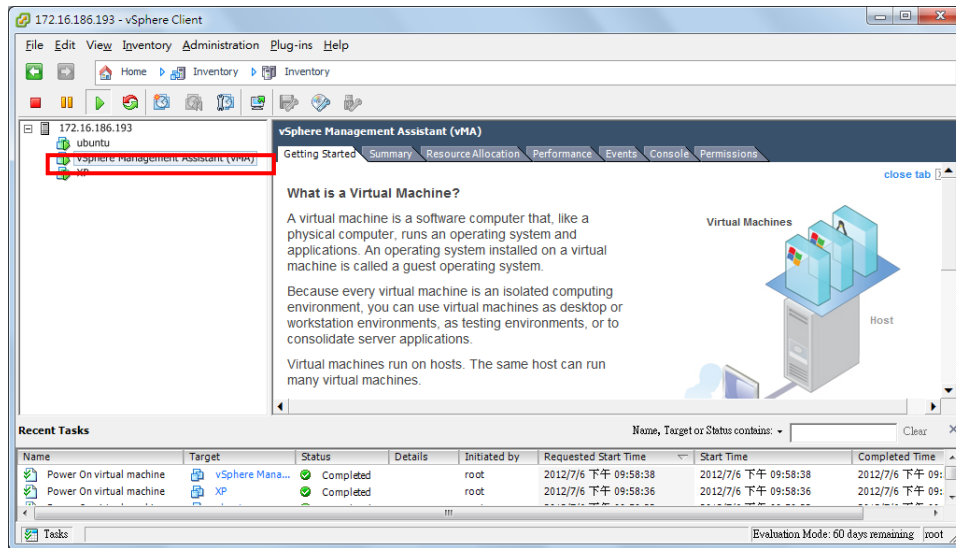
- Shutdown:** A table lists shutdown events with checkboxes for enabling them and input fields for OS shutdown delays. The events listed are Power Fail (300s), Battery Low (30s), and Smart Shutdown (30s).
- Reaction:** Options to 'Notify Message' (60s period) and 'Execute Command File' (with a text area containing '/usr/local/upsagent /command/command.E5X4' and a 'Run Before Shutdown' of 120s).
- Source IP:** Fields for 'Receive Trap Port' (162), 'Purpose' (radio buttons for 'For Redundant (Logical OR)' and 'For Parallel (Logical AND)'), 'Source Trap IP' (192.168.168.239), 'Community' (public), and 'SNMPv3 User'. Below is a table of configured entries.
- Manageable:** A checkbox to 'Allow the ShutdownAgent to be managed by an authenticated manager'.

IP Address	Community	SNMPv3 User
1 192.168.168.239	public	



## 8. Configuration de VMWare ESXi5 pour ShutdownAgent

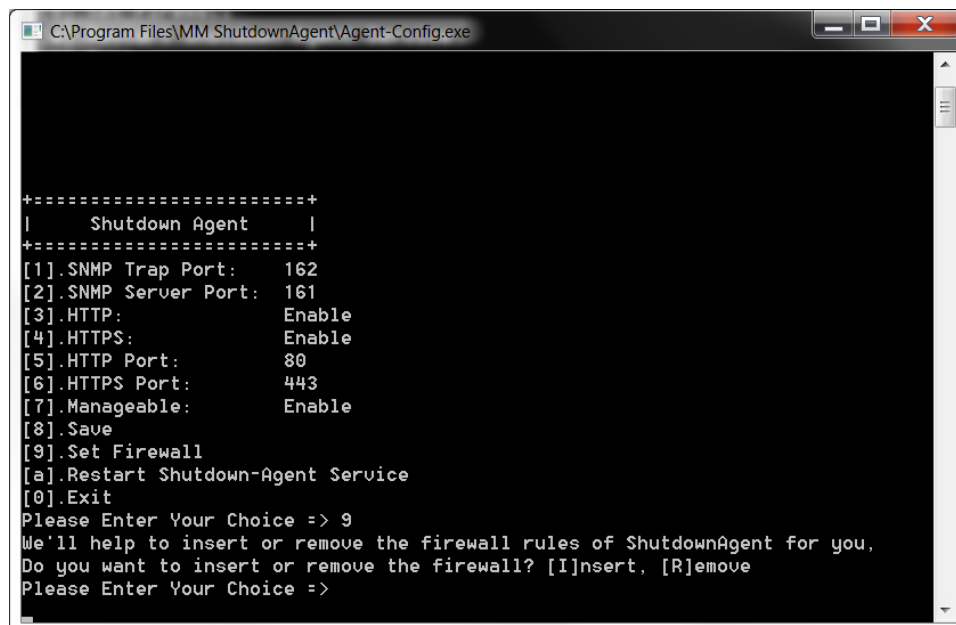
Avant d'installer ShutdownAgent pour ESXi5, vous devez installer le **vMA 5 (assistant de gestion vSphere 5)** et assurez-vous que le **Outils VMware** est installé sur tous les systèmes d'exploitation invités. Transmettez ensuite le fichier d'installation de ShutdownAgent au serveur vMA via SFTP via le client FTP FileZilla ou un autre client SFTP, puis connectez-vous au serveur vMA via la console locale ou via un client SSH (tel que Putty). Suivez la section 2.2 pour l'installation/désinstallation de Linux. Voir le chapitre 3 pour la configuration de la console.



### 8.1 Configurer le pare-feu pour vMA

Exécutez `/usr/local/upsagent/configure`

Sélectionnez [9] pour configurer le pare-feu pour ShutdownAgent.



## 8.2 Installer VMware Tools pour le système d'exploitation invité

Pour arrêter le système d'exploitation invité du serveur ESXi5, installez les outils VMware sur tous les systèmes d'exploitation invités pour effectuer l'arrêt.

Pour le système d'exploitation Windows :

**Sélectionnez le menu suivant Invité - Installer/Mettre à niveau VMware Tools**

## 8.3 Configurer DélimitationAgent pour ESXi5

Entrez le temps estimé pour que tous les systèmes d'exploitation invités qui fonctionnent sur le serveur ESXi5 s'arrêtent correctement.

1. Connectez-vous à l'interface Web de ShutdownAgent. Le niveau du compte doit être égal ou supérieur à celui du gestionnaire de périphériques.
2. Accédez à la page Web Appareil - Hôte - Configurer et entrez le temps estimé dans le champ **Exécuter avant l'arrêt** domaine de la **Réaction** groupe.
3. Entrez **/utilisateur/local/upsagent/commande/commande.ESX5** fichier de script pour ESXi5 pour arrêter les systèmes d'exploitation invités. Cochez ensuite la case Exécuter le fichier de commande pour activer l'arrêt des systèmes d'exploitation invités.
4. Appuyez sur le **Soumettre** bouton pour mettre à jour vos modifications.

The screenshot shows the MM ShutdownAgent web interface. The main content area is titled "Device » Host » Configure". It contains several configuration panels:

- Shutdown:** A table with columns "Enable", "Event", and "OS Shutdown Delay (in seconds)". It lists three events: "Power Fail" (300s), "Battery Low" (30s), and "Smart Shutdown" (30s). A "Submit" button is at the bottom.
- Reaction:** Includes checkboxes for "Notify Message" (checked) and "Execute Command File" (checked). The "Execute Command File" section has a text area containing the command path: `/usr/local/upsagent/command/command.ESX5`. Below it, "Run Before Shutdown" is set to 120 seconds. A "Submit" button is at the bottom.
- Source IP:** Includes "Receive Trap Port" (162), "Purpose" (radio buttons for "For Redundant (Logical OR)" and "For Parallel (Logical AND)"), "Source Trap IP" (192.168.168.239), "Community" (public), and "SNMPv3 User". A table below lists the configuration:
 

IP Address	Community	SNMPv3 User
1 192.168.168.239	public	
- Manageable:** Includes a checkbox "Allow the ShutdownAgent to be managed by an authenticated manager" (checked). A "Submit" button is at the bottom.

Navigation tabs at the top include Monitor, Device, and System. The system time is displayed as Thu 12/13/2012 PM 02:19:30.

## 8.4 Modifier la commande.ESX5

Le script `command.ESX5` doit être configuré pour fournir le nom d'utilisateur et le mot de passe pour que le vMA puisse communiquer avec le serveur ESXi5. Connectez-vous au serveur vMA avec le privilège root et ouvrez le fichier de script suivant avec un programme d'édition de texte :

`/usr/local/upsagent/commande/commande.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-uclicl/apps/um ]; then
# Get the VMware guest OS list
LIST=$(/usr/lib/vmware-uclicl/apps/um/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"
fi
fi
fi

```

Recent Tasks

Name	Target	Status	Details	Initiated by	Requested Start Time	Start Time	Completed Time
[Empty table body]							

Tasks

Evaluation Mode: 60 days remaining root

**NOM D'UTILISATEUR :** le compte racine du serveur ESXi5. **MOT DE PASSE :** le mot de passe du compte root du serveur ESXi5. **SERVERIP :** l'adresse IP du serveur ESXi5.

**LOCALIP :** l'adresse IP du serveur vMA.

Normalement, vous devez fournir le mot de passe root pour le `PASSWORD` et l'adresse IP du serveur ESXi5 pour le `SERVERIP`. Le script obtient automatiquement l'adresse IP vMA de l'interface `eth0`. Si cela ne correspond pas à votre configuration réseau, remplacez-le par l'interface que vous avez créée.

## 9. Configuration de XenServer pour ShutdownAgent

Pour installer ShutdownAgent sur le Citrix XenServer, consultez la section 2.2 pour l'installation/désinstallation de Linux. Pour configurer les paramètres réseau de base, y compris le pare-feu Xen, consultez le chapitre 3 Configuration de la console.

### 9.1 Installer le pilote PV pour le système d'exploitation invité

Pour arrêter le système d'exploitation invité de XenServer, vous devez installer le pilote PV pour tous les systèmes d'exploitation invités.

### 9.2 Configurer DélimitationAgent pour Xen

Entrez le temps estimé nécessaire à l'arrêt correct de tous les systèmes d'exploitation invités fonctionnant sur le XenServer.

1. Connectez-vous à l'interface Web de ShutdownAgent. Le niveau du compte doit être égal ou supérieur à celui du gestionnaire de périphériques.
2. Accédez à la page Web Appareil - Hôte - Configurer et entrez le temps estimé dans le champ **Exécuter avant l'arrêt** domaine de la **Réaction** groupe.
3. Entrer `/utilisateur/local/upsagent/commande/commande.Xen` fichier script pour arrêter les systèmes d'exploitation invités. Cochez ensuite la case Exécuter le fichier de commande pour activer l'arrêt des systèmes d'exploitation invités.
4. Appuyez sur le **Soumettre** bouton pour mettre à jour vos modifications.

The screenshot displays the MM ShutdownAgent web interface. The top navigation bar includes 'Monitor', 'Device', and 'System' tabs, with 'Device' selected. The system time is 'Thu 12/13/2012 PM 02:19:30'. The main content area is titled 'Device » Host » Configure' and contains several configuration panels:

- Shutdown:** A table with columns 'Enable', 'Event', and 'OS Shutdown Delay (in seconds)'. It lists three events: 'Power Fail' (300s), 'Battery Low' (30s), and 'Smart Shutdown' (30s). A 'Submit' button is at the bottom.
- Reaction:** Includes checkboxes for 'Notify Message' (checked, 60s period) and 'Execute Command File' (checked). The command file path is '/usr/local/upsagent/commande/commande.Xen'. A 'Run Before Shutdown' field is set to 120 seconds. A 'Submit' button is at the bottom.
- Source IP:** Includes 'Receive Trap Port' (162), 'Purpose' (radio buttons for 'For Redundant (Logical OR)' and 'For Parallel (Logical AND)'), 'Source Trap IP' (192.168.168.239), 'Community' (public), and 'SNMPv3 User'. A table below lists the configuration:
 

IP Address	Community	SNMPv3 User
1 192.168.168.239	public	
- Manageable:** Includes a checkbox 'Allow the ShutdownAgent to be managed by an authenticated manager' (checked). A 'Submit' button is at the bottom.

## 10. Configuration KVM Linux pour ShutdownAgent

Pour installer ShutdownAgent sur le serveur Linux, voir la section 2.2 Installation/Désinstallation. Pour configurer les paramètres réseau de base, y compris le pare-feu, voir Chapitre 3 Configuration de la console.

### 10.1 Installer les outils libvirt pour KVM

Pour arrêter le système d'exploitation invité du serveur Linux, vous devez installer libvirt. ShutdownAgent appelle le virsh pour arrêter les systèmes d'exploitation invités.

### 10.2 Configurer DélimitationAgent pour KVM

Entrez le temps estimé nécessaire pour que tous les systèmes d'exploitation invités qui fonctionnent sur le serveur KVM s'arrêtent correctement.

1. Connectez-vous à l'interface Web de ShutdownAgent. Le niveau du compte doit être égal ou supérieur à celui du gestionnaire de périphériques.
2. Accédez à la page Web Appareil - Hôte - Configurer et entrez le temps estimé dans le champ **Exécuter avant l'arrêt** domaine de la **Réaction** groupe.
3. Entrez **/utilisateur/local/upsagent/commande/commande.KVM** fichier script pour arrêter les systèmes d'exploitation invités. Cochez ensuite la case Exécuter le fichier de commande pour activer l'arrêt des systèmes d'exploitation invités.
4. Appuyez sur le **Soumettre** bouton pour mettre à jour vos modifications.

**MINUTE MAN**  
POWER TECHNOLOGIES  
By Power Systems, Inc.

**MM ShutdownAgent**

Home Logout

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

Monitor Device System

Host SNMP

Configure

Control

Forward Trap

Device » Host » Configure

**Shutdown**

Shutdown Type: Shutdown

Enable	Event	OS Shutdown Delay (in seconds)
<input checked="" type="checkbox"/>	Power Fail	300 second(s)
<input checked="" type="checkbox"/>	Battery Low	30 second(s)
<input checked="" type="checkbox"/>	Smart Shutdown	30 second(s)

Submit

**Source IP**

Receive Trap Port: 162

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

Submit

Source Trap IP: 192.168.168.239

Community: public

SNMPv3 User:

Add Update Delete

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	

**Reaction**

Notify Message

Period: 60 second(s)

Execute Command File

/usr/local/upsagent  
/command/command.KVM

File:

Run Before Shutdown: 120 second(s)

Submit

**Manageable**

Allow the ShutdownAgent to be managed by an authenticated manager.

Submit

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. Utilisation de la carte SNMP

## 11.1 Carte SNMP-NV6

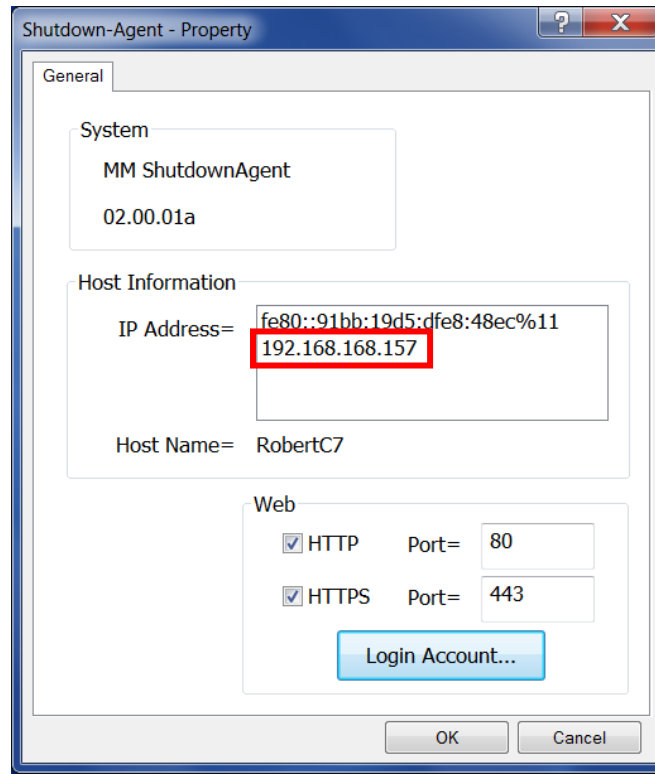
1. Ouvrez un navigateur Web et connectez-vous à la carte SNMP-NV6.
2. Sauvegardez l'adresse IP à partir de la page Web de configuration du système.

The screenshot shows the 'SNMP-NV6 Web' configuration interface. The main content area is titled 'System » Administration » TCP/IP'. It contains two main sections: 'TCP/IP Settings for IPv4' and 'TCP/IP Settings for IPv6'. In the IPv4 section, the 'IP Address' field is set to '192.168.168.239' and is highlighted with a red box. Other fields include Subnet Mask (255.255.255.0), Gateway IP (192.168.168.1), and DNS IP (4.2.2.2). The IPv6 section shows DHCP Client (Disable), IP Address (fe80::230:abff:fe2::), Prefix Length (64), and Gateway V6IP. To the right, the 'System' section shows Host Name (SNMP-NV6), System Contactor (Para), and System Location (CLT4R3). Below that, the 'Link' section has Auto-Negotiation (Enable), Speed (100M), and Duplex (Full). A 'Submit' button is at the bottom right.

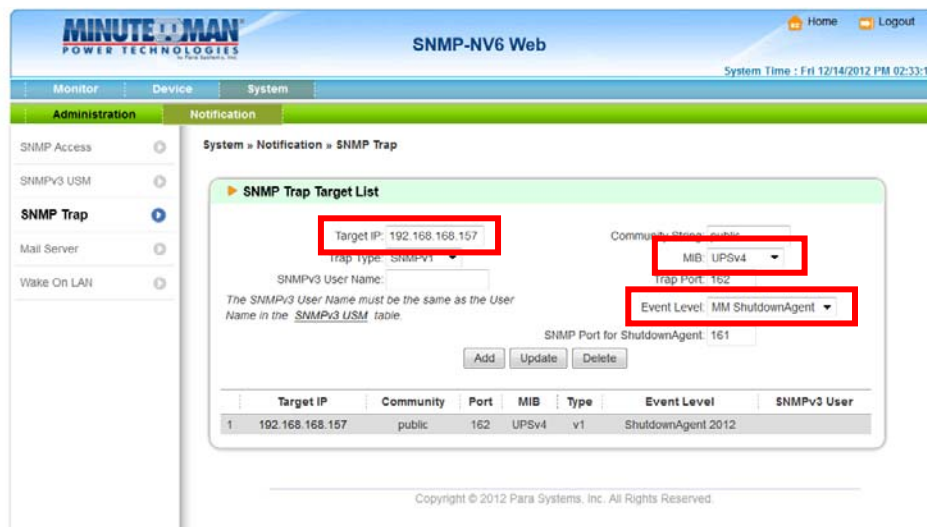
3. Connectez-vous à ShutdownAgent et ajoutez l'adresse IP de la carte SNMP-NV6 et le port de trap pour recevoir le piège SNMP de la carte SNMP-NV6.

The screenshot shows the 'MM ShutdownAgent' configuration interface. The main content area is titled 'Device » Host » Configure'. It contains four main sections: 'Shutdown', 'Source IP', 'Reaction', and 'Manageable'. In the 'Source IP' section, the 'Receive Trap Port' field is set to '162' and the 'Source Trap IP' field is set to '192.168.168.239', both highlighted with red boxes. The 'Shutdown' section shows Shutdown Type (Shutdown) and a table of events with their OS Shutdown Delay. The 'Reaction' section has 'Notify Message' checked with a period of 60 seconds. The 'Manageable' section has 'Allow the ShutdownAgent to be managed by an authenticated manager' checked. A table at the bottom lists the Source IP configuration: IP Address (192.168.168.239) and Community (public).

- Ouvrez la fenêtre des propriétés de ShutdownAgent dans la barre des tâches Windows pour obtenir l'adresse IP du serveur.



- Retournez à la carte SNMP-NV6 et ajoutez l'adresse IP de ShutdownAgent à la table SNMP Trap. Sélectionnez UPSV4 comme Trap MIB et MM ShutdownAgent pour le niveau d'événement.



6. Si vous activez l'option Gérable dans ShutdownAgent, vous pouvez surveiller l'état des ShutdownAgents à partir de la carte SNMP-NV6 (Moniteur >> Informations >> ShutdownAgent).



## 11.2 Carte SNMP-NET

1. Ouvrez un navigateur Web et connectez-vous à la carte SNMP-NET.
2. Sauvegardez l'adresse IP et le port SNMP Trap sur la page Web de configuration du système.
3. Ajoutez l'adresse IP de la carte SNMP-NET et le port Trap au périphérique ShutdownAgent  
>> Hôte >> Page de configuration.
4. Obtenir l'adresse IP de ShutdownAgent à partir de la boîte de dialogue des propriétés.
5. Ajoutez l'adresse IP de ShutdownAgent à la table SNMP Trap de la carte SNMP-NET.
6. Sélectionnez les informations pour le niveau d'événement et MMv4 comme type de MIB d'interruption.