



ShutdownAgent 2012

User Manual

Doc. Version 00.02

Date: 07/06/2012

About this manual

This manual contains information on installation and operation of the ShutdownAgent 2012 software.

Save this Manual

This manual contains instructions and warnings that should be followed during the installation, operation and storage of this product. Failure to heed these instructions and warnings will void the product warranty.

Contents

1. Overview.....	2
1.1 Features	2
1.2 OS Support.....	2
2. Installation/ Uninstallation	4
2.1 For Windows System	4
2.1.1 Installation Process.....	4
2.1.2 Uninstallation Process	7
2.2 For Linux System	8
2.2.1 Installation Process.....	8
2.2.2 Uninstallation Process	9
3. Console Configuration	10
3.1 Console Menu	10
4. Operation in Windows	12
4.1 Web Monitor	12
4.2 Property.....	12
4.3 Show Countdown	15
4.4 Cancel Countdown	15
4.5 Stop Service	15
5. Web Interface	16
5.1 Run a Web Browser	16
5.2 Monitor >> Information >> Summary.....	17
5.3 Monitor >> Information >> Event Log	18
5.4 Monitor >> Information >> Log Configure.....	19
5.5 Device >> Host >> Configure	20
5.6 Device >> Host >> Control	23
5.7 Device >> Host >> Forward Trap	23
5.8 Device >> SNMP >> SNMP Access.....	24
5.9 Device >> SNMP >> SNMPv3 USM.....	25
5.10 System >> Administration >> Information	25
5.11 System >> Administration >> Login User	26
5.12 System >> Administration >> Web	27
5.12 System >> Administration >> Batch Configuration	28
6. 2008 Server Core Setup for ShutdownAgent	29
7. VMWare ESXi4 Setup for ShutdownAgent	31
7.1 Configure the Firewall for ESXi 4	31
7.2 Install VMware Tools for Guest OS	31
7.3 Configure ShutdownAgent for ESXi4	32
8. VMWare ESXi5 Setup for ShutdownAgent	34
8.1 Configure the Firewall for vMA	34
8.2 Install VMware Tools for Guest OS	35

8.3 Configure ShutdownAgent for ESXi5	35
8.4 Modify the Command.ESX5	36
9. XenServer Setup for ShutdownAgent	38
9.1 Install PV driver for Guest OS	38
9.2 Configure UPSentry Cloud for Xen.....	38
10. Linux KVM Setup for ShutdownAgent.....	40
10.1 Install libvirt Tools for KVM.....	40
10.2 Configure ShutdownAgent for KVM.....	40
11. Work with the SNMP Card	42
11.1 Legacy Delta InsightPower SNMP Card.....	42
11.2 New Delta InsightPower SNMP IPv6 Card	44

Linux ubuntu 10.04

Linux Fedora 3.1.9

CentOS 5.8

VMWare ESXi 4.1, 5

Citrix XenServer 6.0.0

Linux KVM

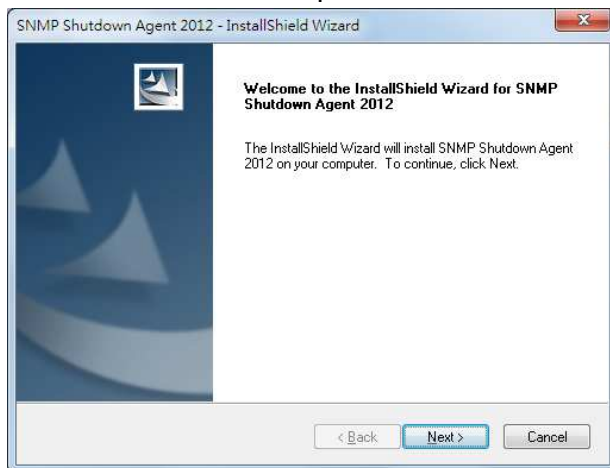
2. Installation/ Uninstallation

2.1 For Windows System

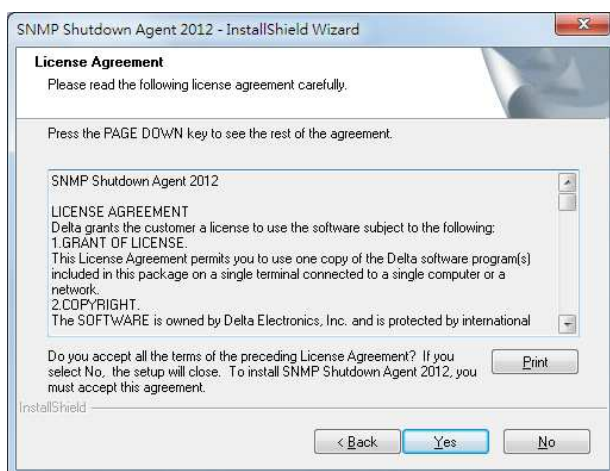
There are 2 of setup programs: ShutdownAgent-2012-Setup(win32).exe and ShutdownAgent-2012-Setup(x64).exe. One is for 32 bit Windows operating system and the other one is designed for 64 bit Windows environment.

2.1.1 Installation Process

1. Execute the ShutdownAgent-2012-Setup(xxx).exe to run the setup program.
2. The welcome page will first display, press the "Next" button to continue the installation or press the "Cancel" to stop the installation.



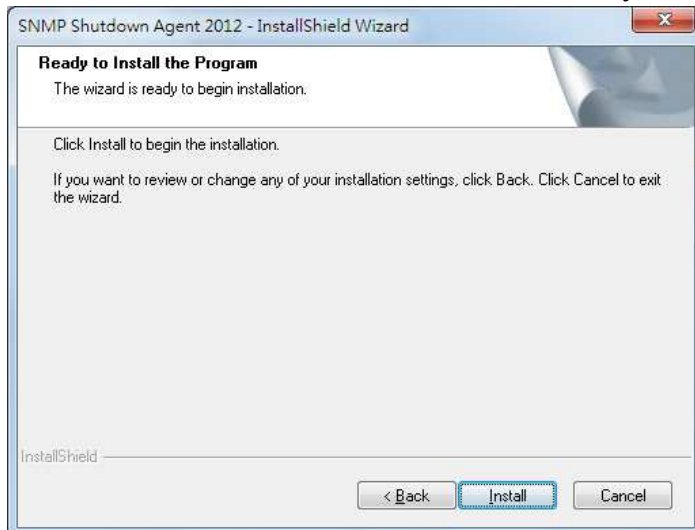
3. Then continue to show the license agreement page. Press "Yes" button to continue the installation and "No" to stop the installation.



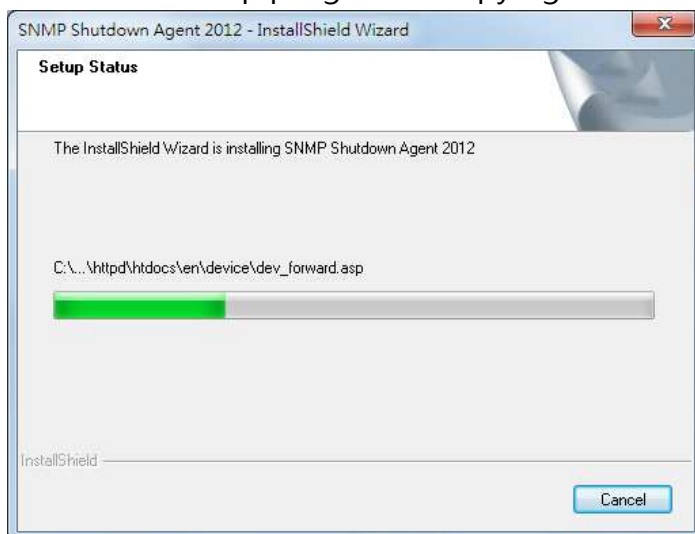
4. At this stage you can change the destination location by pressing the "Browse" button or just press the "Next" to install the software in the default path.



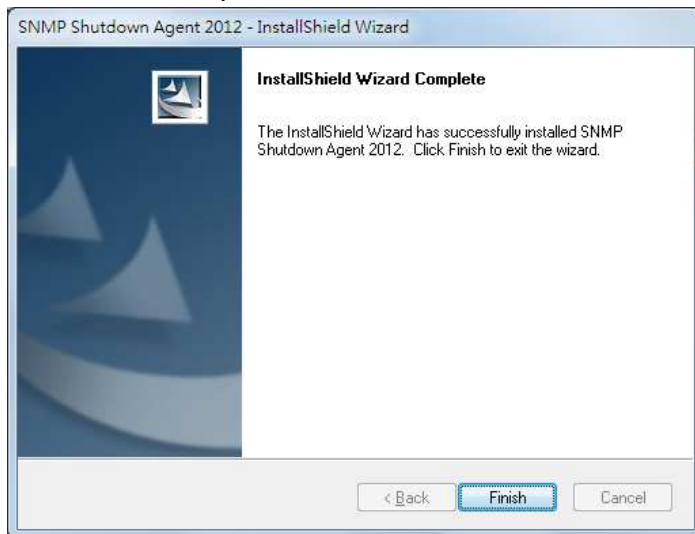
5. Now the setup program is ready for your confirmation to start copying the related program files. Press the "Install" button to start copying the software to the destination location in your hard drive.



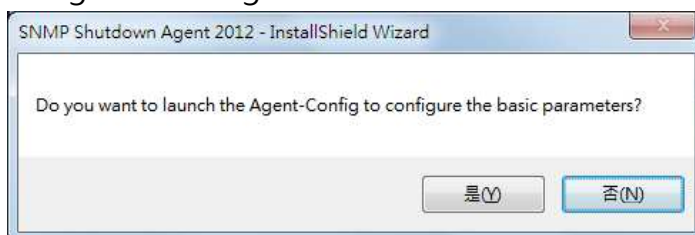
6. Now the setup program is copying the files and shows the progress.



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



8. After finishing the installation, the ShutdownAgent will start the service program automatically and add an icon to indicate its status to the desktop tool bar. Meanwhile, a dialog box pops up to ask for launching the Agent-Config application to do the basic configuration. If you are not operate a Windows server core operating system then you can ignore this ask. Just press “No” to finish the installation. Press “Yes” to launch the Agent-Config in the shell mode. Please refer to the chapter 3 for the detail of Agent-Cofnfig.



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 listen 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 **SNMP ShutdownAgent** association with the following shortcuts:

Console Configure: To launch the Agent-Config.exe for you to quickly configure the basic communication parameters.

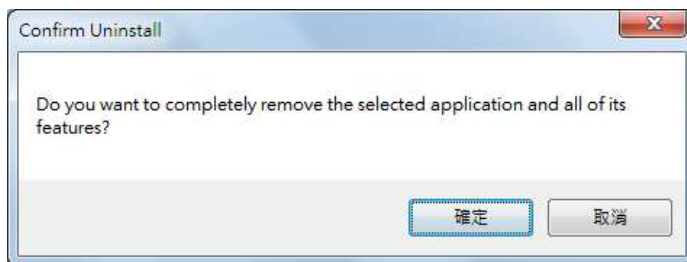
Uninstall: To remove the **SNMP ShutdownAgent 2012** from your hard disk, the configuration data will still be kept in the installed directory.

User Manual: The user manual in pdf format.

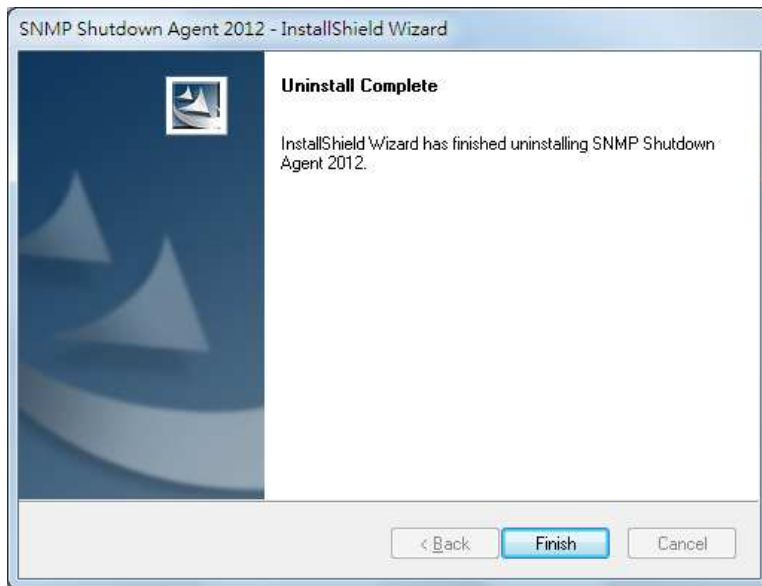
Web Monitor: The major user interface of **ShutdownAgent**, used to monitor and configure the software.

2.1.2 Uninstallation Process

1. Select the Uninstall from the **SNMP ShutdownAgent** program folder to start the un-installation process. Or you can start the **SNMP ShutdownAgent** uninstallation process from the Add/Remove Program of the Control Panel.
2. Press the "OK" button to confirm removing all of the application from the hard drive or "Cancel" to cancel the un-installation process.



3. Press the "Finish" button to complete the un-installation process.



2.2 For Linux System

2.2.1 Installation Process

1. Please login to the Linux system and change to the root account:

```
su root
```

2. Copy the sa2012-linux.tar.gz to the /tmp directory:

```
cp sa2012-linux.tar.gz /tmp
```

3. Change your working directory to /tmp:

```
cd /tmp
```

4. uncompress the sa2012-linux.tar.gz:

```
gunzip sa2012-linux.tar.gz
```

5. extract the sa2012-linux.tar:

```
tar xvf sa2012-linux.tar
```

6. Run the install script:

```
./install
```

```
+-----+
| SNMP ShutdownAgent 2012 0.0.1 for Linux |
| Copyright (c) 2011 Delta Electronics, Inc. |
| All Rights Reserved. |
+-----+
```

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

7. Press 'y' to proceed the installation process:

```

+-----+
| SNMP ShutdownAgent 2012 0.0.1 for Linux |
| Copyright (c) 2011 Delta Electronics, Inc. |
| 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 ShutdownAgent(upsagentd) ... done

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

```

8. Now the ShutdownAgent has been installed in the following directory /usr/local/upsagent/ and the service program starts up automatically. Press 'y' to launch the /usr/local/upsagent/configure program to configure the basic networking parameters for ShutdownAgent or press 'n' to finish the install process.

Please see chapter 3 for more information if you want to configure the basic networking parameters.

2.2.2 Uninstallation Process

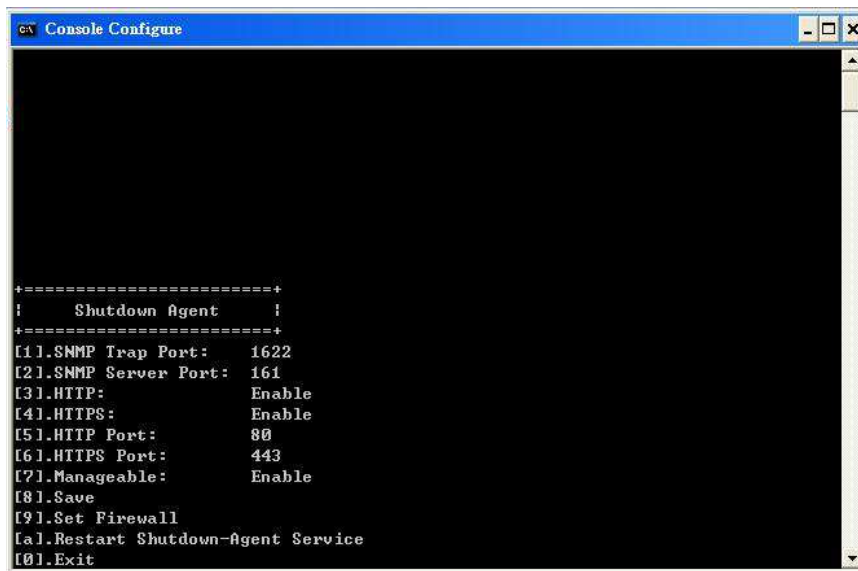
1. Please login to the Linux system and change to the root account:
su root
2. Change your working directory to /usr/local/upsagent:
cd /usr/local/upsagent
3. Run the uninstall script to remove ShutdownAgent:
./uninstall
4. Press 'y' to start the uninstallation process.

3. Console Configuration

The configuration program is design to do the basic configuration for the 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 locates in "C:\Program Files\SNMP Shutdown Agent 2012\Agent-Config.exe"

For Linux it is installed in "/usr/local/upsagent/configure"








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 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 the management software to manage ShutdownAgent	Enable
8.	Save	Save the configured parameters to agent.ini	
9.	Set Firewall	Insert or remove the firewall rule for the	

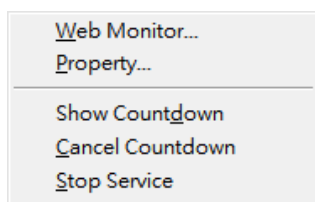
		ShutdownAgent. This option is provided for quickly testing the network communication. The firewall settings may be recovered after the OS reboots.	
a.	Restart Shutdown-Agent Service	Restart service program to apply the changes	
0.	Exit	Exit the configuration program	

4. Operation in Windows

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

Icon	Description
	Normal
	Service stop
	UPS on battery mode
	UPS battery low
	UPS on bypass mode

To show the pop up menu, please move the mouse cursor over the ShutdownAgent icon and click the mouse button to pop up the menu:



4.1 Web Monitor

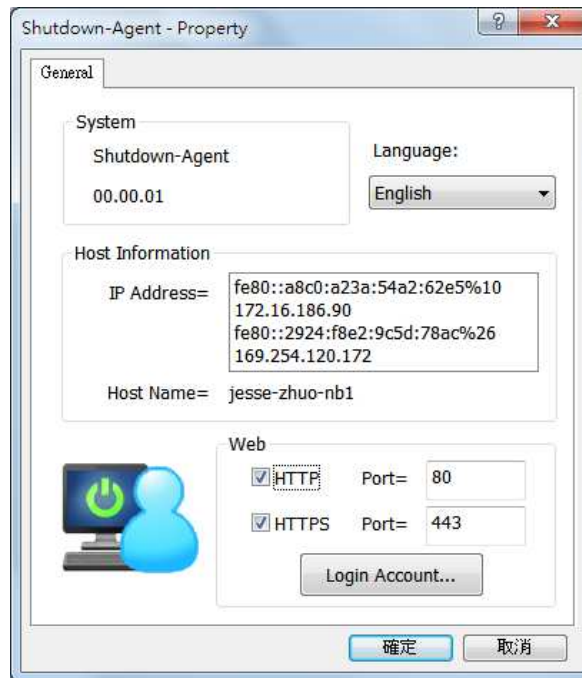
ShutdownAgent implemented a web engine to provide the web interface to interact with the end customers. You can monitor and configure the software through the web interface.

Select the **Web Monitor** menu item from the menu to launch the default web browser, if your login account in the Windows system belongs to the local Administrators group then ShutdownAgent will login to its web engine automatically as the administrator privilege. If you connect a web browser from a remote PC then you have to key in the account and password by yourselves. For more detail information about the web operation, please refer to the chapter 5.

4.2 Property

Select the **Property** menu item will pop-up the Property dialog box which provides another quick way to configure the basic parameters of ShutdownAgent.

From the General page you can observe the software version number, IP addresses and host name.



Language:

Select the supported language from this option.

HTTP:

To enable/ disable the HTTP protocol, assign a different number of the Port number to change the HTTP connection through the other network port. The default value is 80.

If you have changed the HTTP port number from 80 then you have to key in the connection URL as the following:

`http://192.168.1.100:8001`

where 192.168.1.100 is the ip address of the PC which ShutdownAgent installed and the 8001 is the port number which you assigned.

NOTE: Please check the Windows firewall setting if the HTTP connection is refused.

HTTPS:

To enable/ disable support the HTTPS protocol, assign a different number of the Port number to change the HTTPS connection through the other network port. The default value is 443.

If you have changed the HTTPS port number from 443 then you have to key in the connection URL as the following:

`https://192.168.1.100:4430`

where 192.168.1.100 is the ip address of the PC which ShutdownAgent installed and the 4430 is the port number which you assigned.

NOTE: Please 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 the following:

Administrator:

Has sole right to modify the ShutdownAgent system settings.

Device Manager:

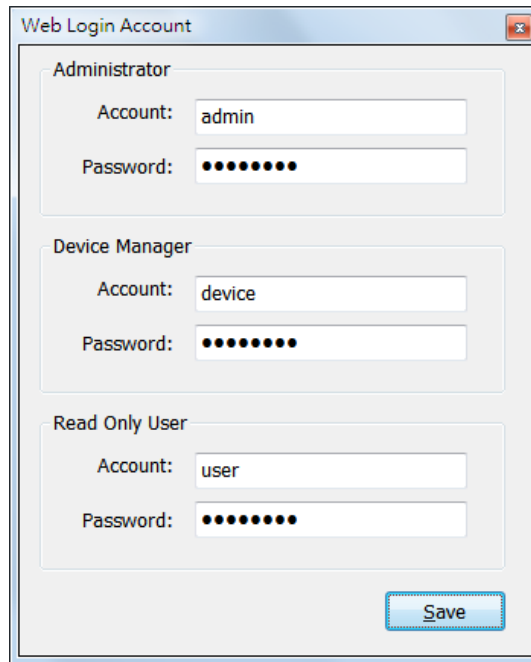
Is not permitted to change the system settings but has the ability to configure the device settings.

Read Only User:

Can observe the connected devices only.

The following is the default account and password list, please note that they are case-sensitive.

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

A screenshot of a 'Web Login Account' dialog box. It contains three sections: 'Administrator' with fields for 'Account' (admin) and 'Password' (masked with dots); 'Device Manager' with fields for 'Account' (device) and 'Password' (masked with dots); and 'Read Only User' with fields for 'Account' (user) and 'Password' (masked with dots). A 'Save' button is located at the bottom right.

4.3 Show Countdown

Select the Show Countdown menu item to display the countdown windows when the ShutdownAgent start to counting down the OS shutdown delay.



4.4 Cancel Countdown

Select the Cancel Countdown menu item during the counting down to stop the shutdown process. To resume the shutdown process, please de-select the Cancel Countdown menu item to counting down the OS shutdown delay.

In addition to de-select the Cancel Countdown menu item to continue the countdown process, when the shutdown event changes the software will start a new countdown process.

4.5 Stop Service

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

5. Web Interface

5.1 Run a Web Browser

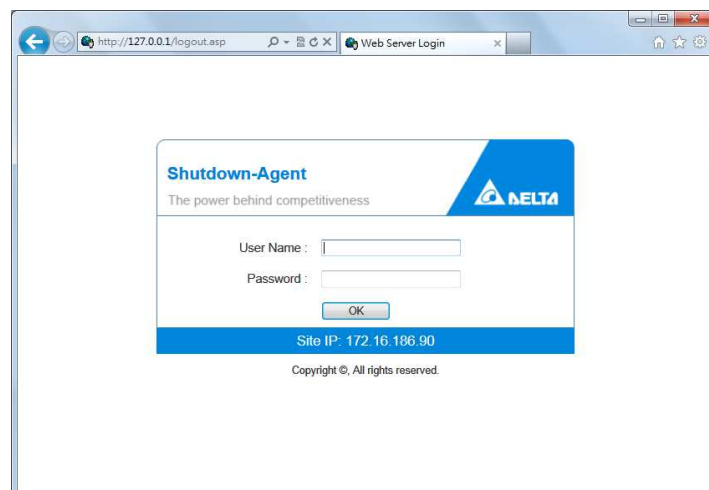
To connect a web browser from the same PC which ShutdownAgent installed, please select the **Web Monitor** from the toolbar menu, ShutdownAgent will open your default web browser and if your Windows account belongs to the local Administrators group then the ShutdownAgent will login as an administrator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

ShutdownAgent allows at most 16 users login at the same time.

You can also connect a web browser from a remote PC, please follow the steps: 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 of HTTP or HTTPS then please 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 your account and password. After keying in the correct **account** and **password**, the **ShutdownAgent Home Page** will appear on the screen.



Note: The ShutdownAgent will logout the user automatically if there is no any data transmission through HTTP/HTTPS for more than 30 minutes.

5.2 Monitor >> Information >> Summary

This web page includes the information of identification, shutdown status, source IP status and the last 5 event logs.

The screenshot shows the Delta SNMP ShutdownAgent 2012 web interface. The browser address bar shows <http://127.0.0.1/home.asp>. The page title is "SNMP ShutdownAgent 2012" with the tagline "The power behind competitiveness". The system time is "Thu 11/24/2011 PM 07:58:08". The navigation menu includes Monitor, Device, and System. The left sidebar has links for Summary, Event Log, and Log Configure. The main content area is titled "Monitor » Information » Summary" and contains three sections:

- Host:** Host Name: jesse-zhuo-nb1, SNMP Trap Port: 162, OS Version: Microsoft Windows 7 Enterprise Edition Service Pack 1 (build 7601), 64-bit.
- Shutdown:** Shutdown Type: Hibernate, OS Countdown: --:--.
- SNMP Trap Source IP List:** Purpose: For Redundant (Logical OR). The table below shows two source IPs with Normal UPS Health.

	Source IP	UPS Health	Current Event
1	10.0.10.21	Normal	
2	172.16.186.162	Normal	

Last 5 Event Log:

	Source IP	Date/Time	Event Level	Event Description
1	Local	11/24/2011 19:56:52	Information	Stop countdown shutdown
2	10.0.10.21	11/24/2011 19:56:52	Information	Power restore
3	Local	11/24/2011 19:56:45	Warning	Countdown to shutdown OS in 04:59 second(s)
4	10.0.10.21	11/24/2011 19:56:45	Warning	Power fail
5	0.0.0.0	11/24/2011 19:55:23	System	Account admin login from 127.0.0.1:50436

Copyright © 2011 Delta Electronics, Inc. All Rights Reserved.

Host:

Include the host name, the listen UDP port for SNMP trap and the description of operating system.

Shutdown:

Display the shutdown type (Shutdown, Power Off, Hibernate) and the countdown time to shutdown the OS in second.

SNMP Trap Source IP List:

ShutdownAgent is capable of receiving SNMP traps from multiple source hosts then decide to determine the event by logical OR for redundant application and logical AND for parallel application.

Last 5 Event Log:

Show the last 5 event logs, if you want to see more please visit the Event Log page.

5.3 Monitor >> Information >> Event Log

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

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 observe the event log by page.

Range of Date:

You can also filter the event log by assigning a period of date. Fill in the From and To text boxes then press the Apply button to request the event log by your assigned period of date.

Download All:

Press the **Download All** button to export all of the event log to a .csv format of file.

The screenshot shows the 'Event Log' page in the SNMP ShutdownAgent 2012 web interface. The page title is 'Monitor » Information » Event Log » Page1'. The left sidebar contains 'Summary', 'Event Log' (selected), and 'Log Configure'. The main content area displays a table of events with columns: IP Address, Date, Time, Level, and Event Log. The table lists various system events, including power restoration, countdowns to shutdown, and service program status changes. A 'Download All' button is located at the top right of the event log table.

IP Address	Date	Time	Level	Event Log
10.0.10.21	11/24/2011	19:56:52	Information	Stop countdown shutdown
10.0.10.21	11/24/2011	19:56:52	Information	Power restore
10.0.10.21	11/24/2011	19:56:45	Warning	Countdown to shutdown OS in 04:59 second(s)
10.0.10.21	11/24/2011	19:56:45	Warning	Power fail
	11/24/2011	19:55:23	System	Account admin login from 127.0.0.1:50436
	11/24/2011	19:55:00	System	IPv4-Trap: OK, IPv6-Trap: OK
	11/24/2011	19:55:00	System	IPv4-SNMP: OK, IPv6-SNMP: OK
	11/24/2011	19:54:55	System	IPv4-HTTP: OK, IPv6-HTTP: OK, IPv4-HTTPS: OK, IPv6-HTTPS: OK
	11/24/2011	19:54:55	System	Service program startup
10.0.10.21	11/24/2011	19:41:07	Information	Stop countdown shutdown
10.0.10.21	11/24/2011	19:41:06	Information	Power restore
10.0.10.21	11/24/2011	19:40:54	Warning	Countdown to shutdown OS in 04:54 second(s)
10.0.10.21	11/24/2011	19:40:54	Warning	Power fail
	11/24/2011	19:38:34	System	Account admin login from 127.0.0.1:15735
	11/24/2011	19:36:05	System	IPv4-Trap: OK, IPv6-Trap: OK
	11/24/2011	19:36:05	System	IPv4-SNMP: OK, IPv6-SNMP: OK
	11/24/2011	19:36:00	System	IPv4-HTTP: OK, IPv6-HTTP: OK, IPv4-HTTPS: OK, IPv6-HTTPS: OK
	11/24/2011	19:36:00	System	Service program startup
	11/24/2011	19:35:52	System	Service program is terminated
	11/24/2011	19:33:22	System	Account admin login from 127.0.0.1:46340
	11/24/2011	19:26:20	System	IPv4-Trap: OK, IPv6-Trap: OK
	11/24/2011	19:26:20	System	IPv4-SNMP: OK, IPv6-SNMP: OK
	11/24/2011	19:26:15	System	IPv4-HTTP: OK, IPv6-HTTP: OK, IPv4-HTTPS: OK, IPv6-HTTPS: OK
	11/24/2011	19:26:15	System	Service program startup
	11/24/2011	19:23:53	System	IPv4-Trap: OK, IPv6-Trap: OK
	11/24/2011	19:23:53	System	IPv4-SNMP: OK, IPv6-SNMP: OK
	11/24/2011	19:23:48	System	IPv4-HTTP: OK, IPv6-HTTP: OK, IPv4-HTTPS: OK, IPv6-HTTPS: OK

5.4 Monitor >> Information >> Log Configure

This page lets the Device Manager clear event log.

Clear Event Log:

To clear all of the data log by clicking this button.

The screenshot shows the 'Log Configure' page in the SNMP ShutdownAgent 2012 web interface. The page title is 'Monitor » Information » Log Configure'. The left sidebar contains 'Summary', 'Event Log', and 'Log Configure' (selected). The main content area displays a box with the text 'Maximum event log entry: 10000' and a 'Clear Event Log' button. The footer contains the copyright notice: 'Copyright © 2011 Delta Electronics, Inc. All Rights Reserved.'

5.5 Device >> Host >> Configure

This page is used to configure the major functions, they are: Shutdown, Reaction and Source IP.

Shutdown:

Select the **Shutdown Type** to determine the way to shutdown the operating system. There are **Shutdown**, **Power Off** and **Hibernate** types and the default value is Shutdown.

Now we should continue to determine the shutdown delay time for the following 4 power events: Power Fail, Battery Low, Overload and Smart Shutdown. If the power events recover during countdown then the operating system will not be shutdown.

The screenshot displays the 'SNMP ShutdownAgent 2012' web interface. The breadcrumb trail is 'Device > Host > Configure'. The 'Shutdown' section is active, showing a 'Shutdown Type' dropdown set to 'Shutdown'. Below it is a table for configuring shutdown delays:

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"/>	Overload	60 second(s)
<input checked="" type="checkbox"/>	Smart Shutdown	30 second(s)

The 'Reaction' section has two options: 'Notify Message' (checked, with a period of 60 seconds) and 'Execute Command File' (checked, with the command 'c:\windows\notepad.exe' and a delay of 300 seconds). The 'Manageable' section has a checkbox 'Allow the ShutdownAgent to be managed by an authenticated manager' which is checked. The 'Source IP' section on the right shows 'Receive Trap Port: 162', 'Purpose' set to 'For Redundant (Logical OR)', 'Source Trap IP: 10.0.10.33', and 'Community: public'. A table at the bottom lists the Source IP configuration:

IP Address	Community	SNMPv3 User
10.0.10.33	public	

Reaction:

Enable the **Notify Message** to pops up a message box once ShutdownAgent receives the SNMP traps from the source IP addresses. Assign the period value to report the message periodically, set a 0 to the Period will show the message only once.

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

Source IP:

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

Redundant(Logical OR): Summarize the received power event by logical OR for all of the source IP addresses to determine whether the power event occurs or not. So if the power event occurs 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 the ShutdownAgent stops countdown and cancel the shutdown process.

Parallel(Logical AND): Summarize the received power event by logical AND for all of the source IP addresses to determine whether the power event occurs or not. So if the power event occurs 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 stops countdown and cancel the shutdown process.

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

Community: If the value is not empty then only the received trap with the same community string will be accepted. If the value is empty then ShutdownAgent will accept any of the received community string.

SNMPv3 User: This field is used for SNMPv3 packet. If the value is not empty then only the received trap with the same user defined in the

SNMPv3 USM table will be accepted. If the value is empty then ShutdownAgent will accept the users which assigned in the SNMPv3 USM table.

Manageable:

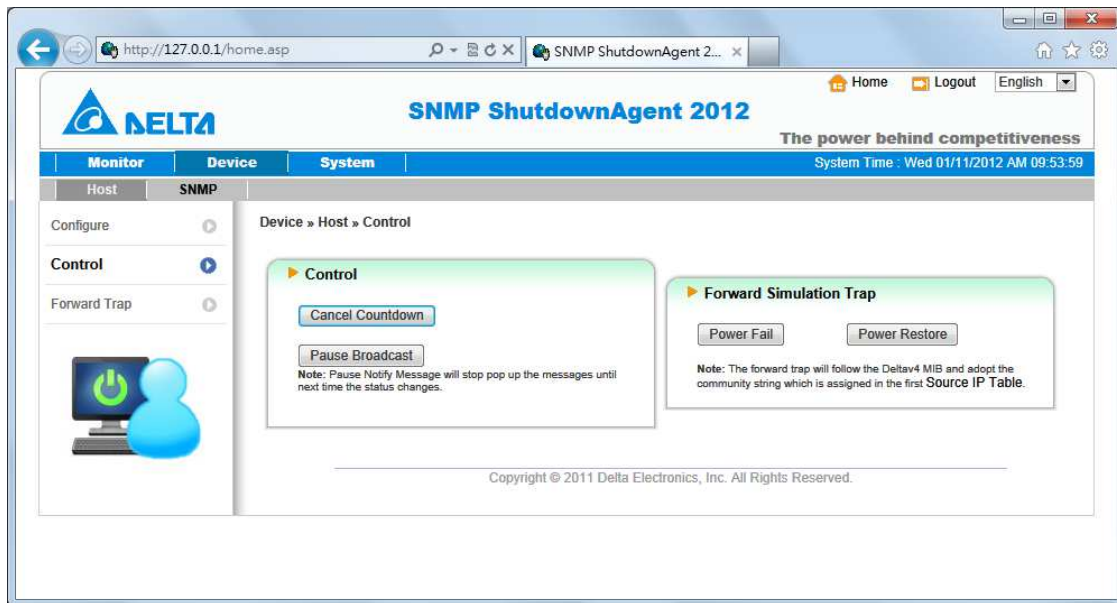
Select the **Allow the ShutdownAgent to be managed by an authenticated manager** option to let the ShutdownAgent reply the query from any authenticated manager. The authenticated manager can be a SNMP card or a centralized management software. After collecting the ShutdownAgent information, the authenticated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

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

In fact, the authenticated manager communicate with the ShutdownAgent through SNMPv3 with the first default account in the SNMPv3 USM list. If the **Allow the ShutdownAgent to be managed by an authenticated manager** option is enabled then the permission of "manager" account changes to "Read/Write", otherwise the permission is "Disable".

The default setting of **Allow the ShutdownAgent to be managed by an authenticated manager** option is "enabled".

5.6 Device >> Host >> Control



Control:

Press the Cancel Countdown button during the countdown shutdown process to stop counting down. 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.

5.7 Device >> Host >> Forward Trap

Forward Trap is used to forward the received SNMP trap to extend the size of protection OS shutdown gracefully.



5.8 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 that are allowed to access, their community strings and access levels. The maximum number of IP entries is 255.



5.9 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 whose access is granted via SNMPv3 protocol. You can also define their respective Security Levels, Auth Passwords, Priv Passwords and Permission.

The first one account cannot be deleted, to disable it please go to the Device >> Host >> Configure web page then uncheck the manageable option.

The screenshot shows the web interface for SNMP ShutdownAgent 2012. The browser address bar shows `http://127.0.0.1/home.asp`. The page title is "SNMP ShutdownAgent 2012" with the tagline "The power behind competitiveness". The system time is "Wed 01/11/2012 AM 10:11:46".

The navigation menu includes "Monitor", "Device", and "System". Under "Device", there are "Host" and "SNMP" sub-menus. The "SNMP" menu is selected, and the "SNMPv3 USM" option is highlighted in the sidebar.

The main content area is titled "Device » SNMP » SNMPv3 USM". It contains a form for adding or updating a user. The form fields are:

- Context Name: `cn1027`
- Auth Protocol: `MD5`
- Priv Protocol: `CBC-DES`
- User Name: `jesse`
- Security Level: `Auth, Priv` (dropdown)
- Auth Password: `*****`
- Priv Password: `*****`
- Permission: `Read Only` (dropdown)

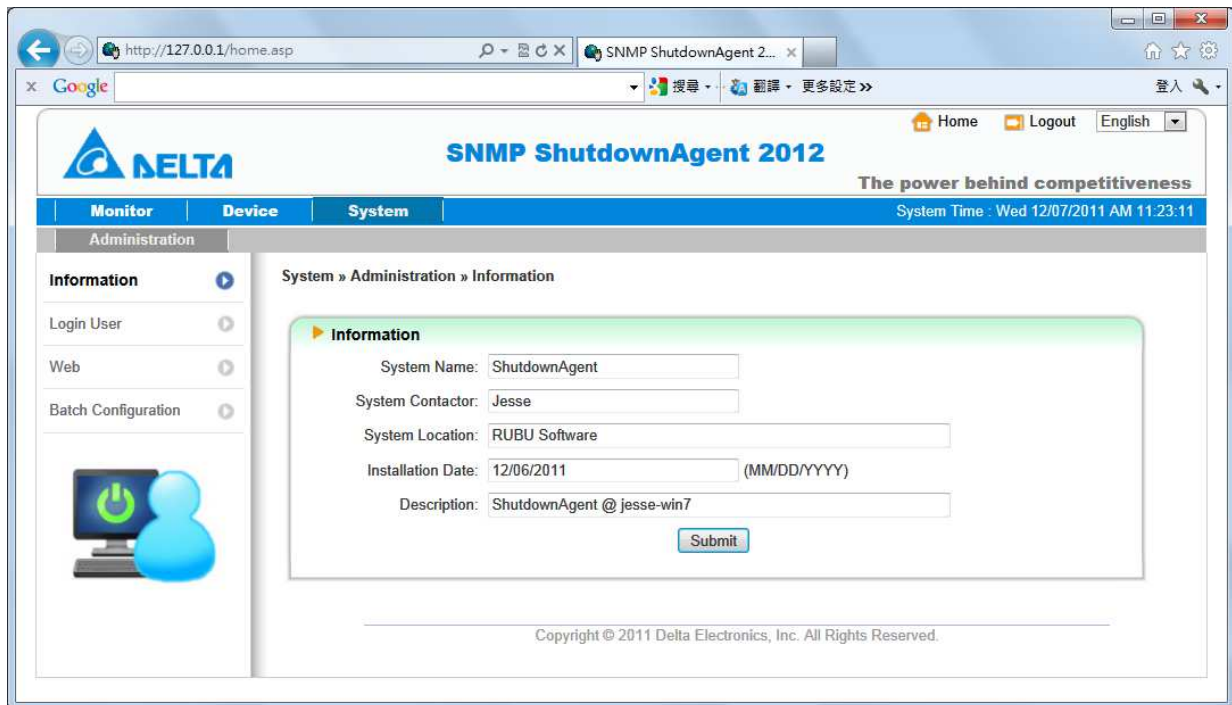
Buttons for "Submit", "Add", "Update", and "Delete" are present. Below the form is a table listing the configured users:

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

Copyright © 2011 Delta Electronics, Inc. All Rights Reserved.

5.10 System >> Administration >> Information

Here to assign the system information for the ShutdownAgent, including Installation Date, Location and Description.



5.11 System >> Administration >> Login User

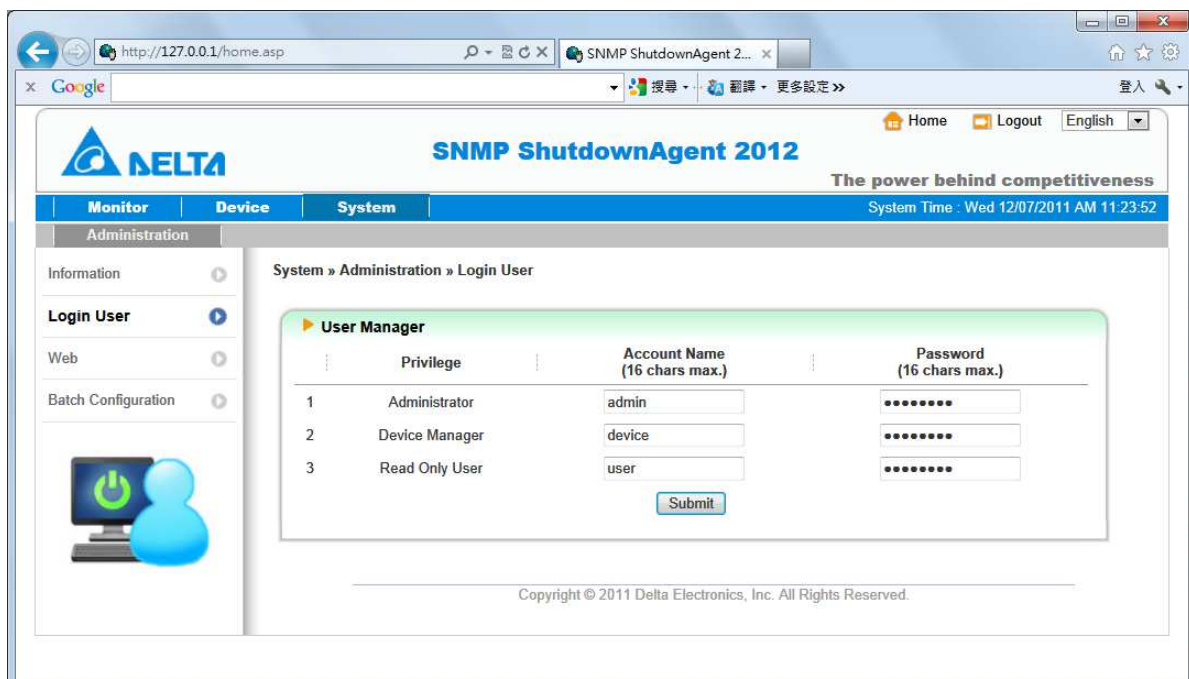
You can manage the login authentication for web interface by assigning 3 different level of users' account and password.

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

Administrator: Permitted to modify all settings.

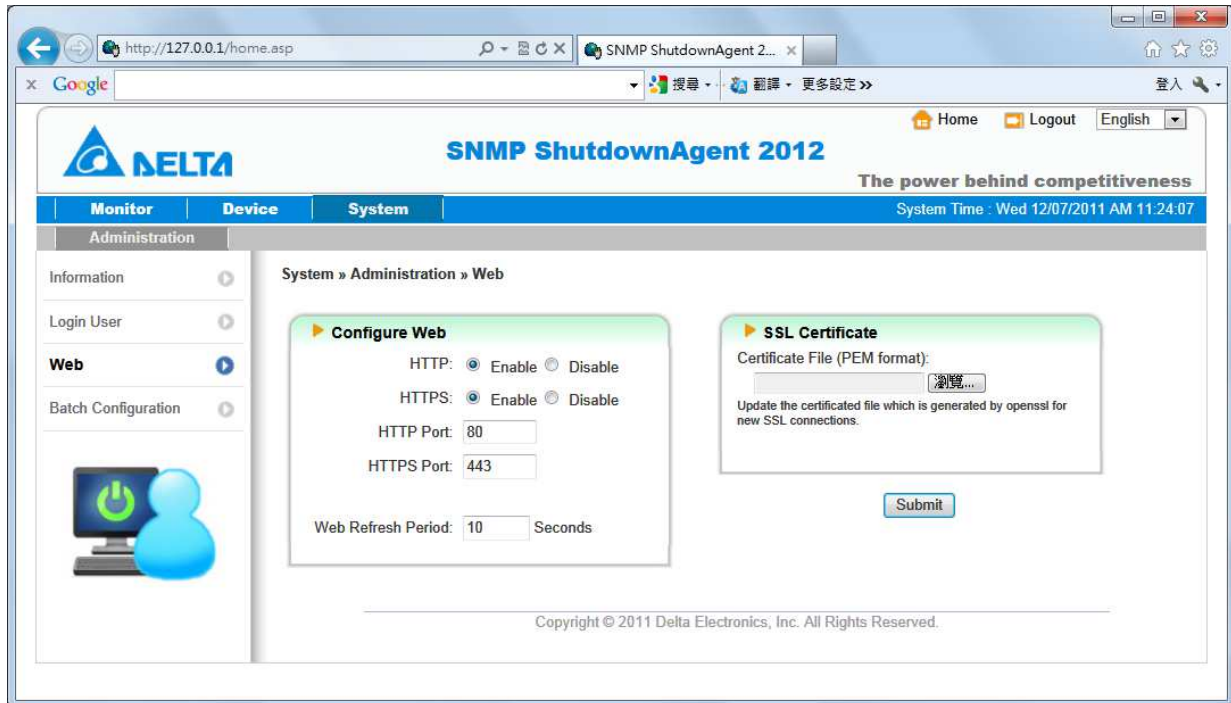
Device Manager: Permitted to modify device-related settings.

Read Only User: Only permitted to observe ShutdownAgent status.



5.12 System >> Administration >> Web

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



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 period of time to update the monitoring web pages. The range is 1~9999 seconds.

SSL Certificate:

To ensure connection security between the ShutdownAgent and the

connecting workstation, SSL certificate can be used to encrypt and secure the integrity of transmitting 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 a certificate file.

5.12 System >> Administration >> Batch Configuration

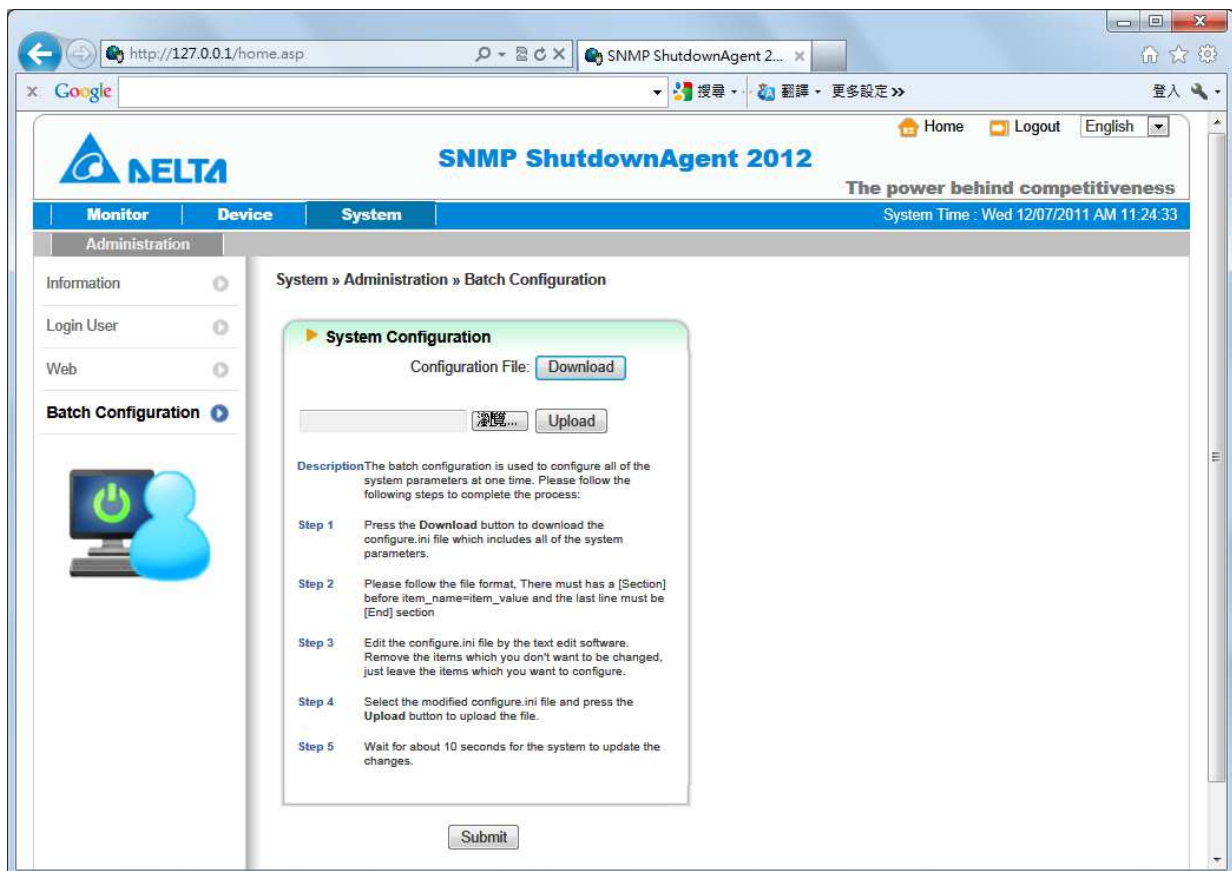
The ShutdownAgent provides batch configuration to allow quick and effortless setup on multiple ShutdownAgent hosts. You can duplicate settings by downloading the configuration file from the ShutdownAgent that you have successfully configured, and upload the configuration files on other hosts.

Download:

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

Upload:

Upload the configuration file to ShutdownAgent to apply the change immediately.



6. 2008 Server Core Setup for ShutdownAgent

While installation the ShutdownAgent in the 2008 server core, it requires the following commands to transfer the file and add some rules for firewall.

1. Disable firewall:

```
netsh advfirewall set allprofiles state off
```

2. Enable 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 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 HTTPS TCP 443

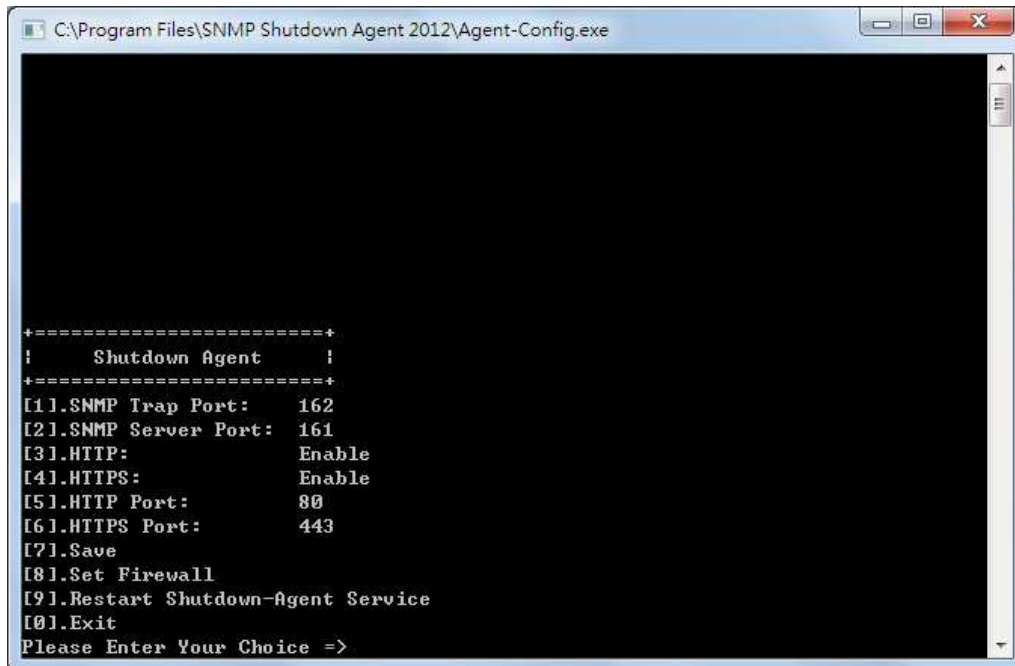
```
netsh advfirewall firewall add rule name="HTTPS" protocol=TCP dir=in localport=443  
action = allow
```

Firstly, 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. Don't forget to set the "Enable firewall" command when complete.

Secondly, follow the chapter 2 to install the ShutdownAgent in the 2008 server.

The last step is use the open HTTP/HTTPS, SNMP Trap/Server port commands to open the necessary which you want.

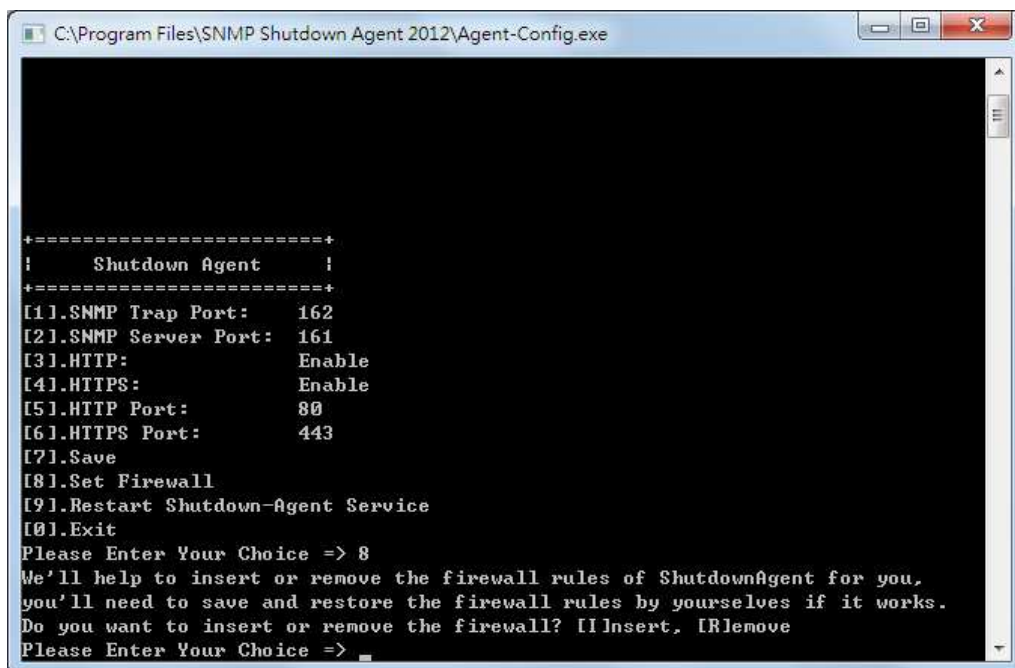
You can easily run the Agent-Config.exe to configure the basic networking parameters for the web and SNMP network protocols after installation.



```
C:\Program Files\SNMP Shutdown Agent 2012\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].Save
[8].Set Firewall
[9].Restart Shutdown-Agent Service
[0].Exit
Please Enter Your Choice =>
```

Select [8] to help you to insert or remove a firewall rule for the ShutdownAgent.



```
C:\Program Files\SNMP Shutdown Agent 2012\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].Save
[8].Set Firewall
[9].Restart Shutdown-Agent Service
[0].Exit
Please Enter Your Choice => 8
We'll help to insert or remove the firewall rules of ShutdownAgent for you,
you'll need to save and restore the firewall rules by yourselves if it works.
Do you want to insert or remove the firewall? [I]Insert, [R]Remove
Please Enter Your Choice => _
```

7. VMWare ESXi4 Setup for ShutdownAgent

Before installing the ShutdownAgent in the ESXi4 server, please transmit the ShutdownAgent setup file to the ESX server through SFTP by FileZilla FTP Client or other SFTP client then login to the ESX server by the local console or through your favorite SSH client (such as Putty).

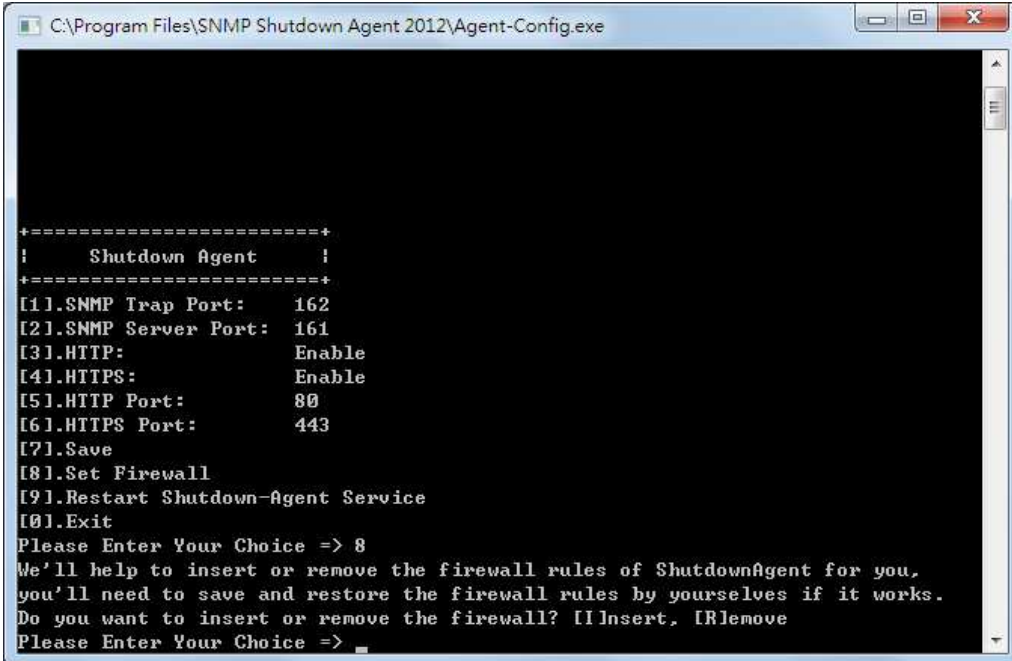
Please continue to follow the section 2.2 For Linux Installation/ Uninstallation.

To configure the basic networking parameters including the ESXi4 firewall, please see chapter 3 Console Configuration.

7.1 Configure the Firewall for ESXi 4

Run the /usr/local/upsagent/configure

Select [8] to help you to insert or remove a firewall rule for the ShutdownAgent.



```

C:\Program Files\SNMP Shutdown Agent 2012\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].Save
[8].Set Firewall
[9].Restart Shutdown-Agent Service
[10].Exit
Please Enter Your Choice => 8
We'll help to insert or remove the firewall rules of ShutdownAgent for you,
you'll need to save and restore the firewall rules by yourselves if it works.
Do you want to insert or remove the firewall? [I]Insert, [R]remove
Please Enter Your Choice =>
  
```

7.2 Install VMware Tools for Guest OS

To shutdown the guest OS from ESXi server, it's better for you to install the VMware tools for all of them so as to inform the guest OSes shutdown smoothly.

For Windows operating system.

Select the following menu Guest → Install/Upgrade VMware Tools

7.3 Configure ShutdownAgent for ESXi4

The only thing that you need to do is to estimate the period of time during shutdown all of the guest operating systems which run in the ESXi4 server. Then

1. Login to the web interface of ShutdownAgent and the account level should greater than or equal to device manager.
2. Goto the Device → Host → Configure web page and fill the estimated time in the **Run Before Shutdown** field of the **Reaction** group.

The screenshot shows the web interface of ShutdownAgent 2012. The browser address bar shows `http://10.0.10.25/home.asp`. The page has a sidebar on the left and a main content area. In the main content area, there is a 'Reaction' section with a green header. It contains a 'Notify Message' checkbox (checked), a 'Period' field set to 60 seconds, an 'Execute Command File' checkbox (unchecked), and a 'File' field containing `/usr/local/upsagent/command/command.ESX5`. Below these is a 'Run Before Shutdown' field set to 120 seconds, which is highlighted with a red rectangular box. To the right of the 'Reaction' section is a 'Manageable' section with a green header, containing a checkbox 'Allow the ShutdownAgent to be managed by an authenticated manager' (checked) and a 'Submit' button. Above the 'Manageable' section is a table with columns 'IP Address', 'Community', and 'SNMPv3 User', containing one row with values '10.0.10.33', 'public', and an empty field respectively. At the top of the main content area, there is a 'Smart Shutdown' section with a checkbox (checked) and a 'Submit' button.

3. We have built the **command.ESX4** script file for ESXi 4 to shutdown the guest OSes, please change the file name in the Execute Command File field to the **command.ESX4** then check the Execute Command File checkbox to enable shutdown the guest OSes.

This screenshot shows the same web interface as the previous one, but with changes. In the 'Reaction' section, the 'Execute Command File' checkbox is now checked. The 'File' field now contains `/usr/local/upsagent/command/command.ESX4`. The 'Run Before Shutdown' field remains at 120 seconds. The 'Manageable' section and the table above it are unchanged. The 'Smart Shutdown' section at the top is also unchanged.

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

The screenshot shows the ShutdownAgent 2012 web interface. The browser address bar displays `http://10.0.10.25/home.asp`. The page title is "SNMP ShutdownAgent 2012". The navigation menu on the left includes "Host", "SNMP", "Configure", "Control", and "Forward Trap". The main content area is titled "Device » Host » Configure".

Shutdown Section:

Shutdown Type:

	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"/>	Overload	60 second(s)
4	<input checked="" type="checkbox"/>	Smart Shutdown	30 second(s)

Reaction Section:

☒ Notify Message
Period: 60 second(s)

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

Source IP Section:

Receive Trap Port:

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

Source Trap IP:
Community:
SNMPv3 User:

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

	IP Address	Community	SNMPv3 User
1	10.0.10.33	public	

Manageable Section:

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

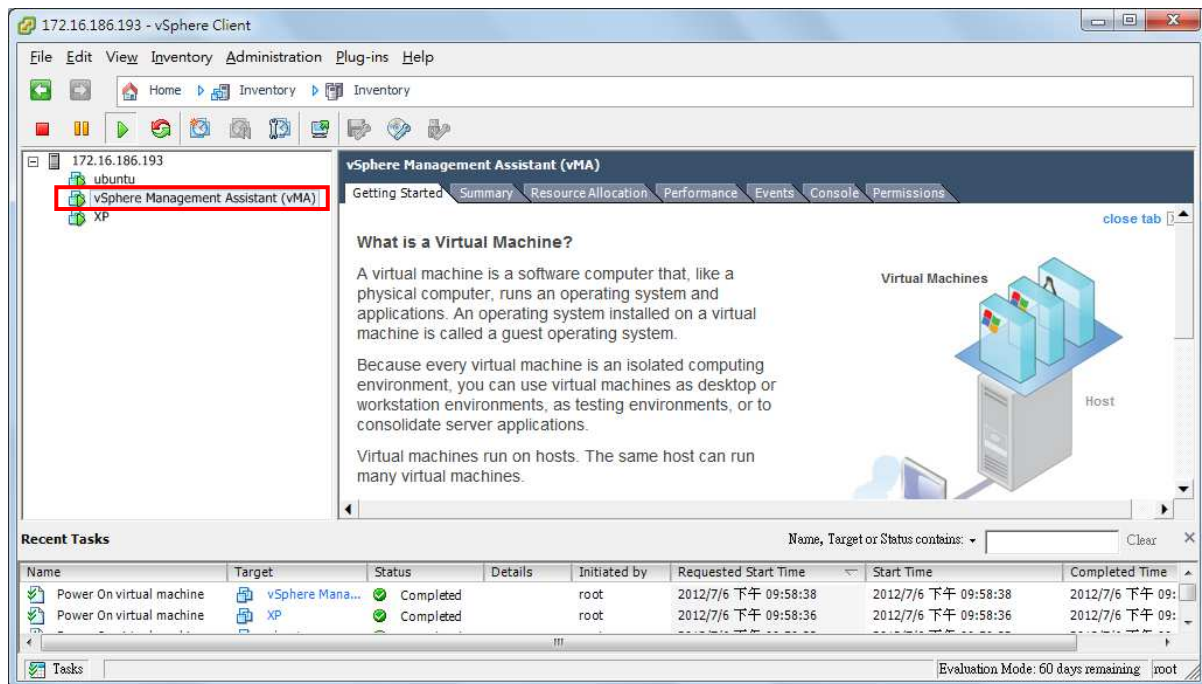
Note: The authenticated manager can be a SNMP card or a centralized management software. Enable this option to integrate the ShutdownAgent in the power management environment.

8. VMWare ESXi5 Setup for 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 in all of the guest OSes. Please then transmit the ShutdownAgent setup file to the vMA server through SFTP by FileZilla FTP Client or other SFTP client then login to the vMA server by the local console or through your favorite SSH client (such as Putty).

Please continue to follow the section 2.2 For Linux Installation/ Uninstallation.

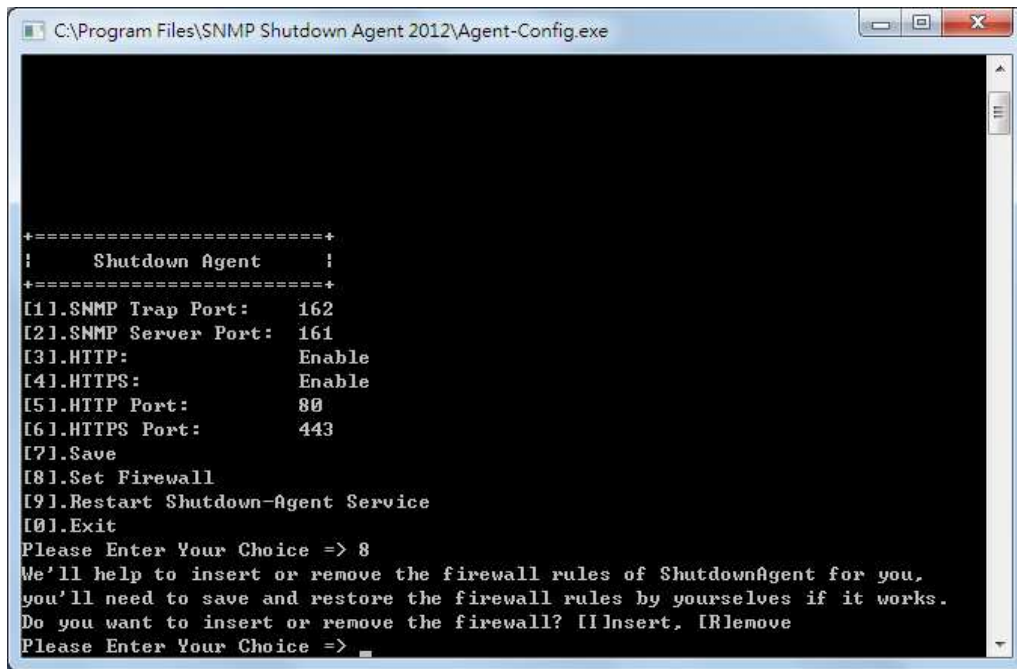
To configure the basic networking parameters including the vMA firewall, please see chapter 3 Console Configuration.



8.1 Configure the Firewall for vMA

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

Select [8] to help you to insert or remove a firewall rule for the ShutdownAgent.



8.2 Install VMware Tools for Guest OS

To shutdown the guest OS from ESXi5 server, you have to install the VMware tools for all of them so as to inform the guest OSes shutdown smoothly.

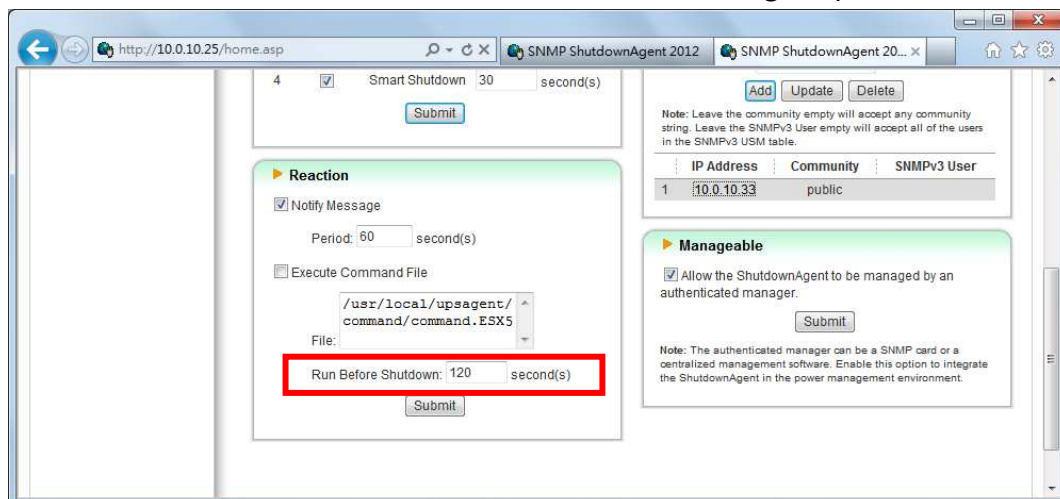
For Windows operating system.

Select the following menu Guest → Install/Upgrade VMware Tools

8.3 Configure ShutdownAgent for ESXi5

Please estimate the period of time during shutdown all of the guest operating systems which run in the ESXi5 server. Then

1. Login to the web interface of ShutdownAgent and the account level should greater than or equal to device manager.
2. Goto the Device → Host → Configure web page and fill the estimated time in the **Run Before Shutdown** field of the **Reaction** group.



3. We have built the **command.ESX5** script file for ESXi 5 to shutdown the guest OSES, please make sure the file name in the Execute Command File field is **command.ESX5** then check the Execute Command File checkbox to enable shutdown the guest OSES and ESXi5 server.

The screenshot shows the 'Smart Shutdown' configuration page. The 'Execute Command File' checkbox is checked and highlighted with a red box. The file path is set to `/usr/local/upsagent/command/command.ESX5`. The 'Run Before Shutdown' is set to 120 seconds. The 'Submit' button is visible at the bottom of the configuration section.

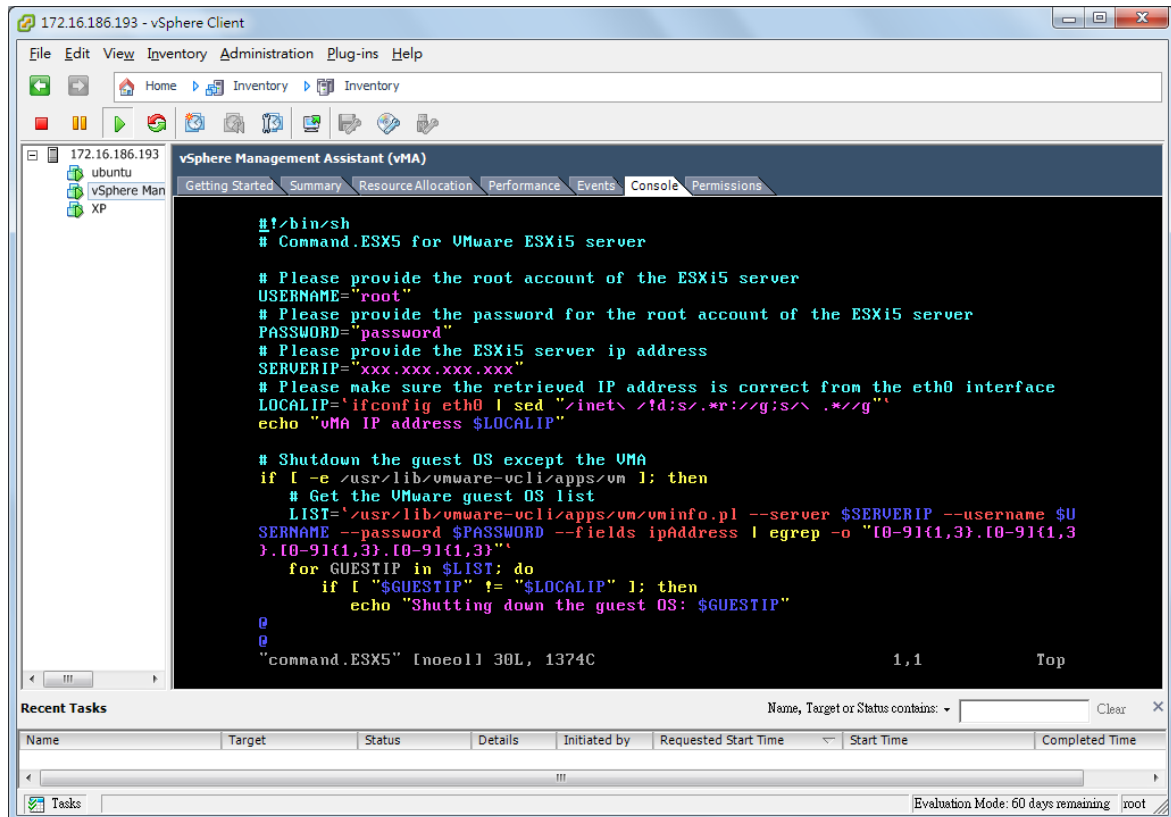
4. Press **Submit** button to update your changes.

The screenshot shows the 'Smart Shutdown' configuration page. The 'Execute Command File' checkbox is checked and highlighted with a red box. The file path is set to `/usr/local/upsagent/command/command.ESX5`. The 'Run Before Shutdown' is set to 120 seconds. The 'Submit' button is visible at the bottom of the configuration section.

8.4 Modify the Command.ESX5

It is required for the customer to modify the **command.ESX5** script to provide the user name, password for the vMA to communicate with the ESXi5 server.

Please login to the vMA server, open the following script file by a text edit with the root privilege: /usr/local/upsagent/command/command.ESX5.



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 with your network configuration please change it to the interface which you have created.

9. XenServer Setup for ShutdownAgent

To install the ShutdownAgent in the Citrix XenServer, please see 2.2 For Linux in chapter 2 Installation/ Uninstallation.

To configure the basic networking parameters including the Xen firewall, please see chapter 3 Console Configuration.

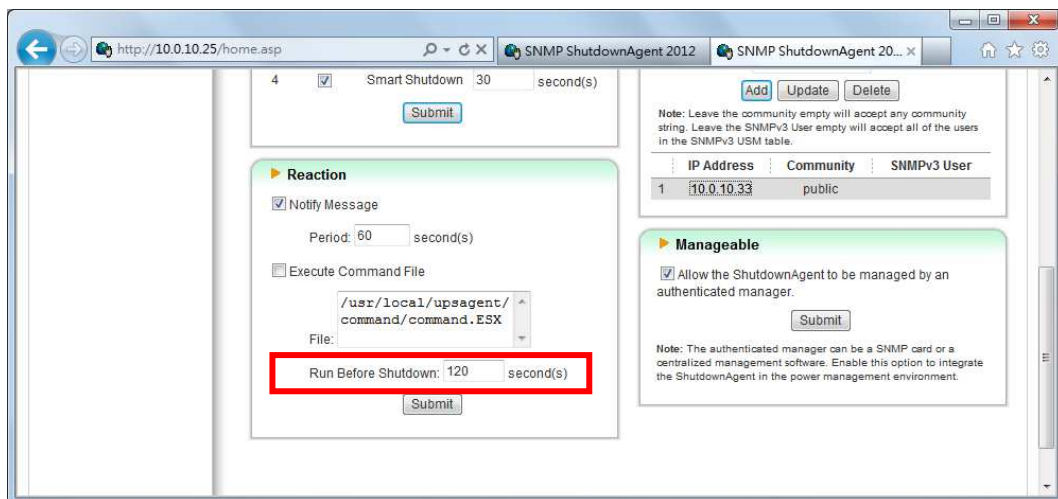
9.1 Install PV driver for Guest OS

To shutdown the guest OS from XenServer, you need to install the PV driver for all of them so as to inform the guest OSes shutdown smoothly.

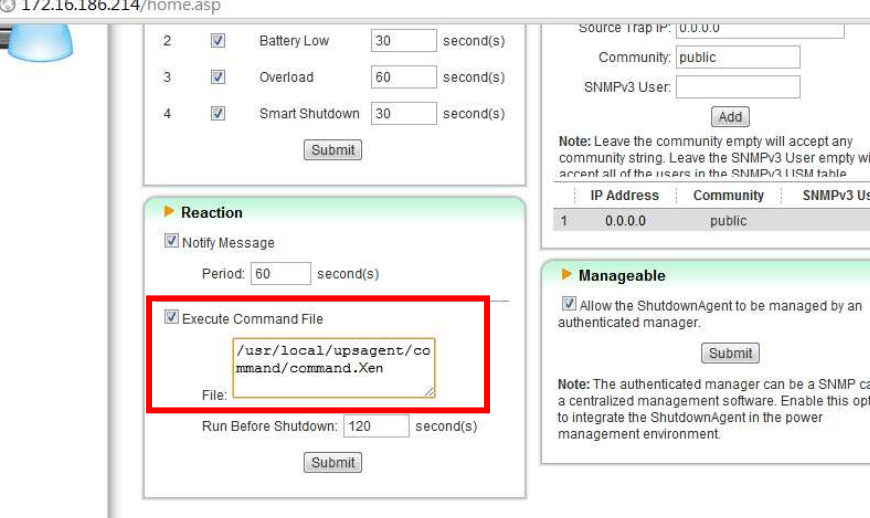
9.2 Configure UPSentry Cloud for Xen

The only thing that you need to do is to estimate the period of time during shutdown all of the guest operating systems which run in the XenServer. Then

1. Login to the web interface of ShutdownAgent and the account level should be greater than or equal to device manager.
2. Go to the Device → Host → Configure web page and fill the estimated time in the **Run Before Shutdown** field of the **Reaction** group.



3. We have built the **command.Xen** script file to shutdown the guest OSes, so you have to change the file name from command.ESX to command.Xen in the Execute Command File. Please then check the Execute Command File checkbox to enable shutdown the guest OSes.



SNMP ShutdownAgent 2.0

172.16.186.214/home.asp

2 ☒ Battery Low 30 second(s)

3 ☒ Overload 60 second(s)

4 ☒ Smart Shutdown 30 second(s)

Reaction

☒ Notify Message

Period: 60 second(s)

☒ Execute Command File

`/usr/local/upsagent/command/command.Xen`

File:

Run Before Shutdown: 120 second(s)

Source Trap IP: 0.0.0.0

Community: public

SNMPv3 User:

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

	IP Address	Community	SNMPv3 User
1	0.0.0.0	public	

Manageable

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

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

Copyright © 2012 Delta Electronics, Inc. All Rights Reserved.

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

10. Linux KVM Setup for ShutdownAgent

To install the ShutdownAgent in the Linux server, please see 2.2 For Linux in chapter 2 Installation/ Uninstallation.

To configure the basic networking parameters including the firewall, please see chapter 3 Console Configuration.

10.1 Install libvirt Tools for KVM

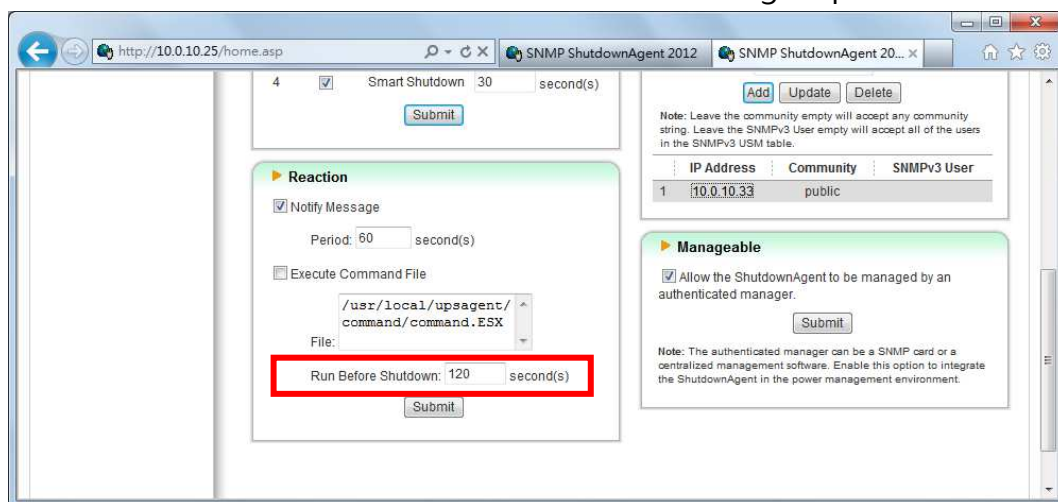
To shutdown the guest OS from Linux server, you have to install the libvirt. ShutdownAgent calls the virsh to shutdown the running guest OSes.

10.2 Configure ShutdownAgent for KVM

The only thing that you need to do is to estimate the period of time during shutdown all of the guest operating systems which run in the KVM server.

Then

1. Login to the web interface of ShutdownAgent and the account level should greater than or equal to device manager.
2. Goto the Device → Host → Configure web page and fill the estimated time in the **Run Before Shutdown** field of the **Reaction** group.



3. We have built the **command.KVM** script file to shutdown the guest OSes, so you have to change the file name from `command.ESX` to `command.KVM` in the Execute Command File. Please then check the Execute Command File checkbox to enable shutdown the guest OSes.

SNMP ShutdownAgent 2012

172.16.186.214/home.asp

2 ☒ Battery Low 30 second(s)

3 ☒ Overload 60 second(s)

4 ☒ Smart Shutdown 30 second(s)

Reaction

☒ Notify Message

Period: 60 second(s)

☒ Execute Command File

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

Run Before Shutdown: 120 second(s)

Source Trap IP: 0.0.0.0

Community: public

SNMPv3 User:

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

IP Address	Community	SNMPv3 User
1 0.0.0.0	public	

Manageable

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

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

Copyright © 2012 Delta Electronics, Inc. All Rights Reserved.

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

SNMP ShutdownAgent 2012

172.16.186.214/home.asp

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"/>	Overload	60 second(s)
<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.KVM`

Run Before Shutdown: 120 second(s)

Source IP

Receive Trap Port: 162

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

Source Trap IP: 0.0.0.0

Community: public

SNMPv3 User:

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

IP Address	Community	SNMPv3 User
1 0.0.0.0	public	

Manageable

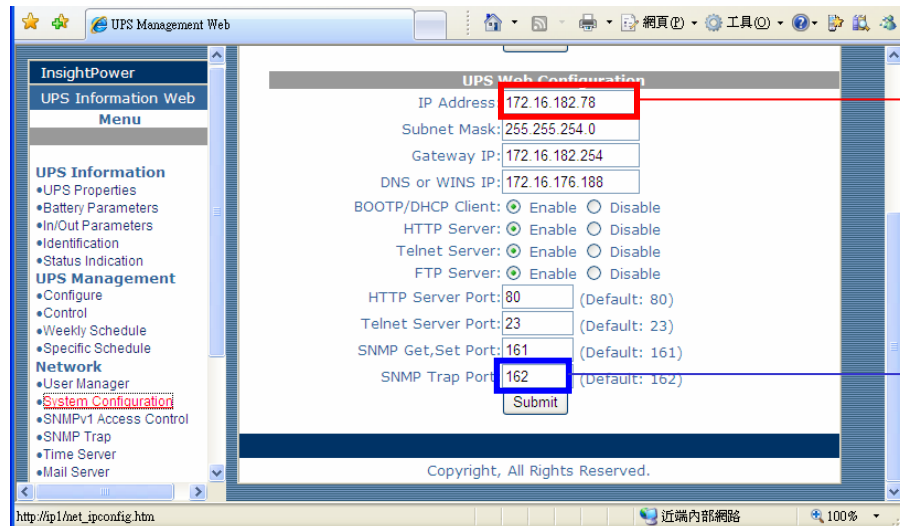
☒ Allow the ShutdownAgent to be managed by an authenticated manager.

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

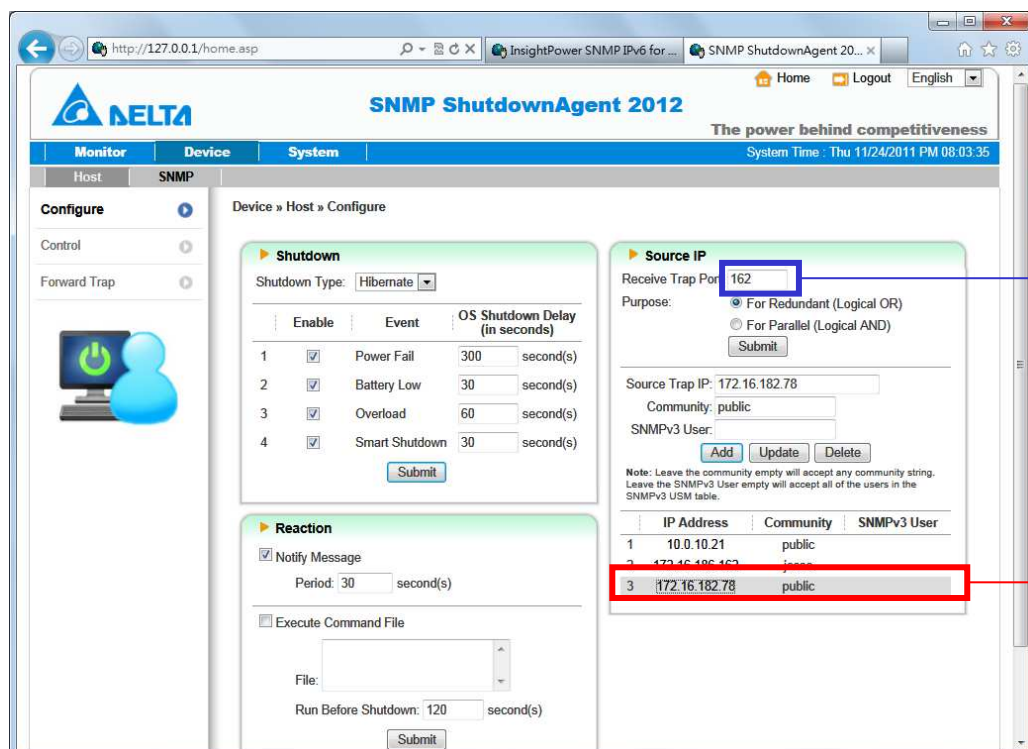
11. Work with the SNMP Card

11.1 Legacy Delta InsightPower SNMP Card

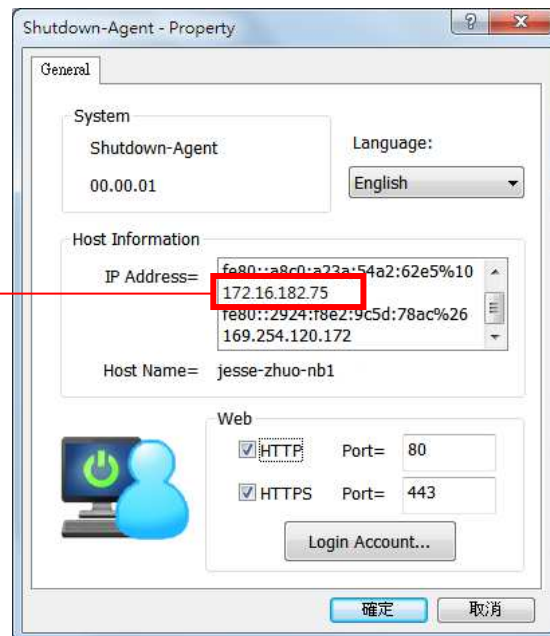
1. Open a web browser and connect to the InsightPower SNMP Card.
2. Record the IP address and SNMP Trap Port in the System Configuration web page.



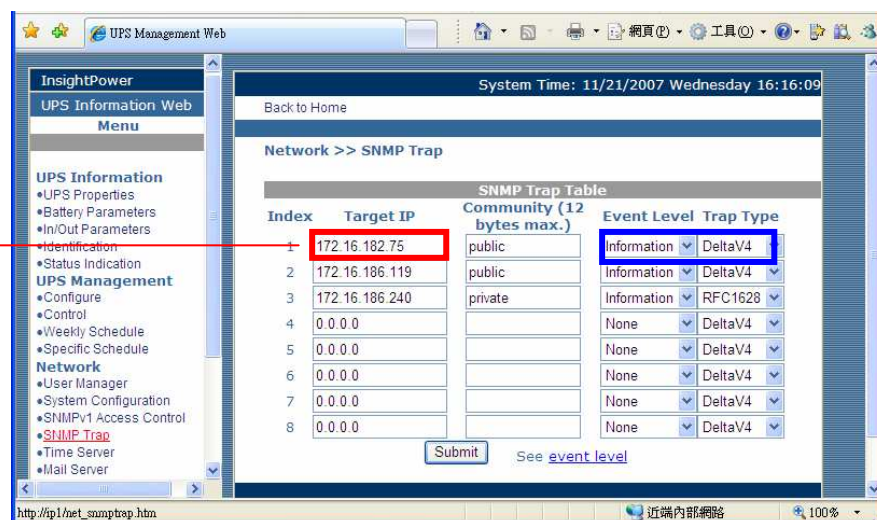
3. Add the SNMP IP address and the trap port to the ShutdownAgent as the following to receive the SNMP trap from the InsightPower SNMP Card.



4. Get the ShutdownAgent ip address form the property dialog box.

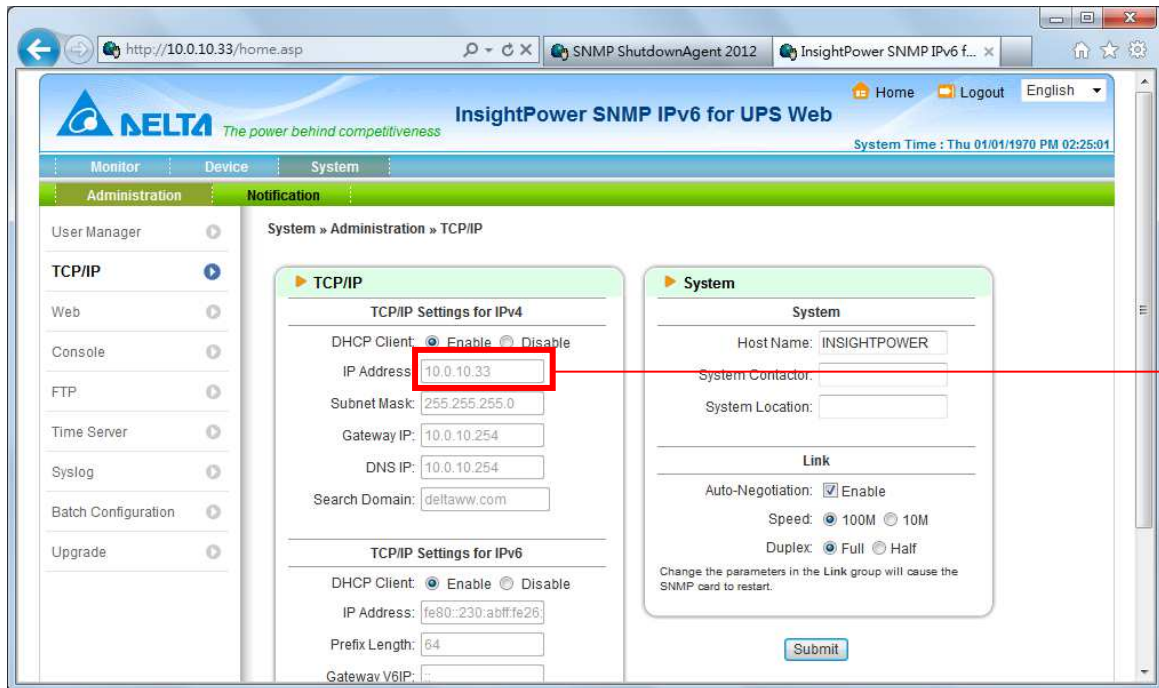


5. Add the ShutdownAgent ip address to the SNMP Trap table in the InsightPower SNMP Card. Please select the "Information" for the Event Level and DeltaV4 as the Trap MIB Type.

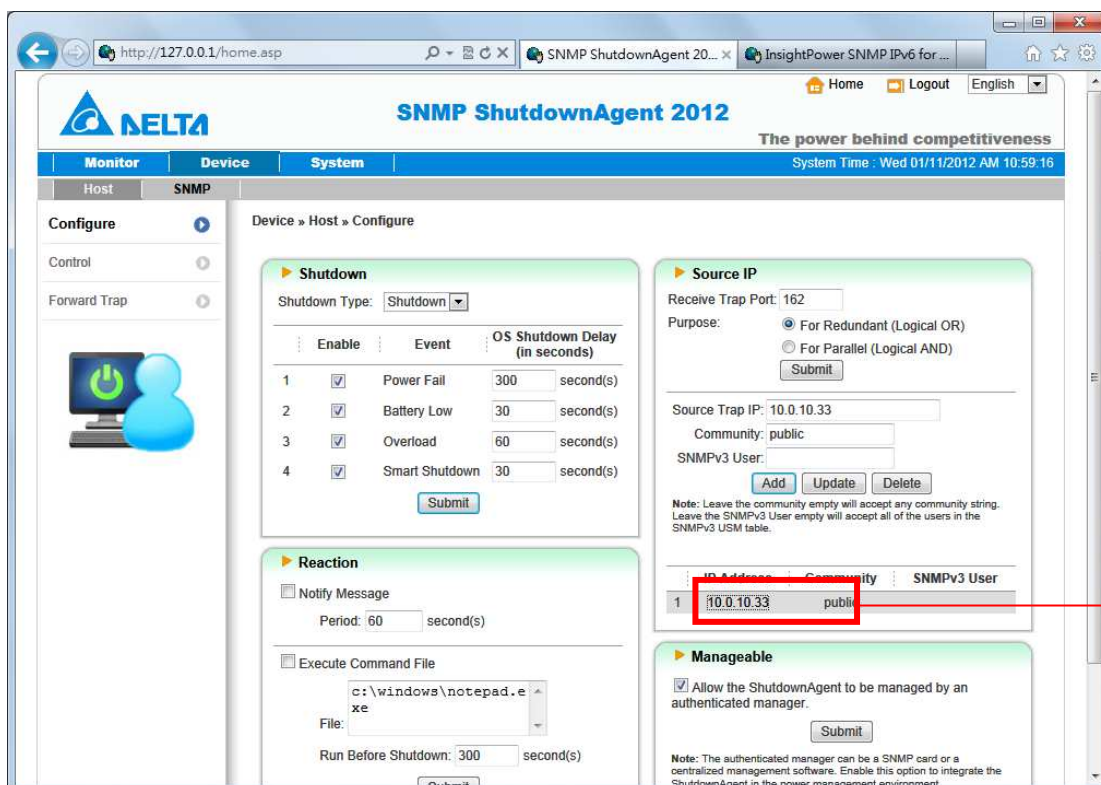


11.2 New Delta InsightPower SNMP IPv6 Card

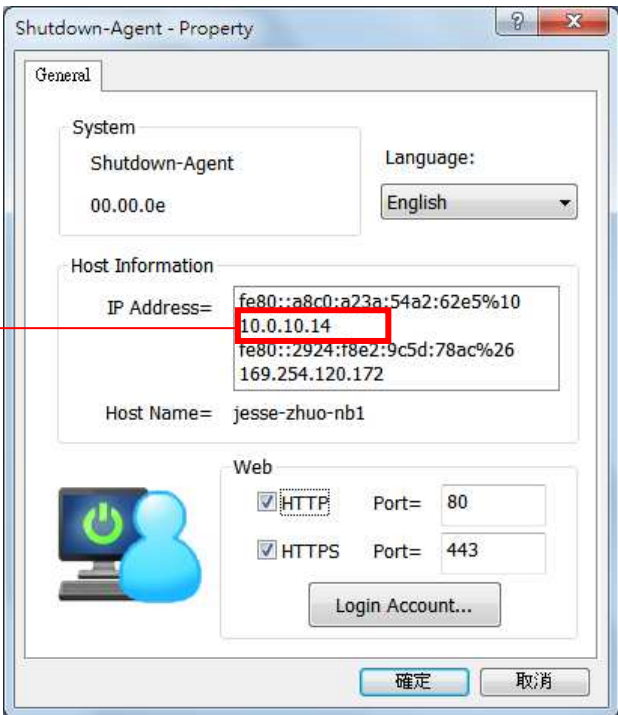
1. Open a web browser and connect to the InsightPower SNMP IPv6 Card.
2. Record the IP address in the System Configuration web page. The SNMP Trap is assigned in the SNMP Trap web page individually.



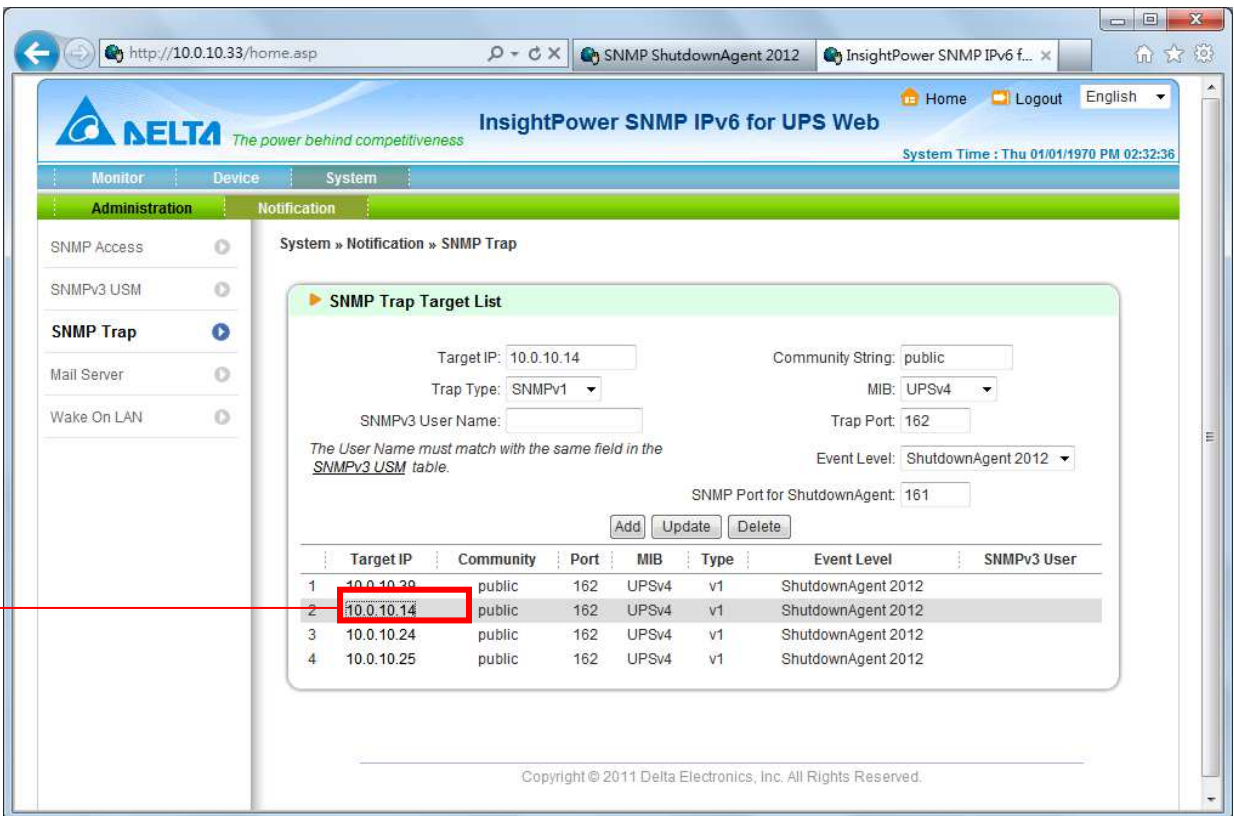
3. Login to the ShutdownAgent web and add the SNMP IP address and the trap port as the following to receive the SNMP trap from the SNMP Card.



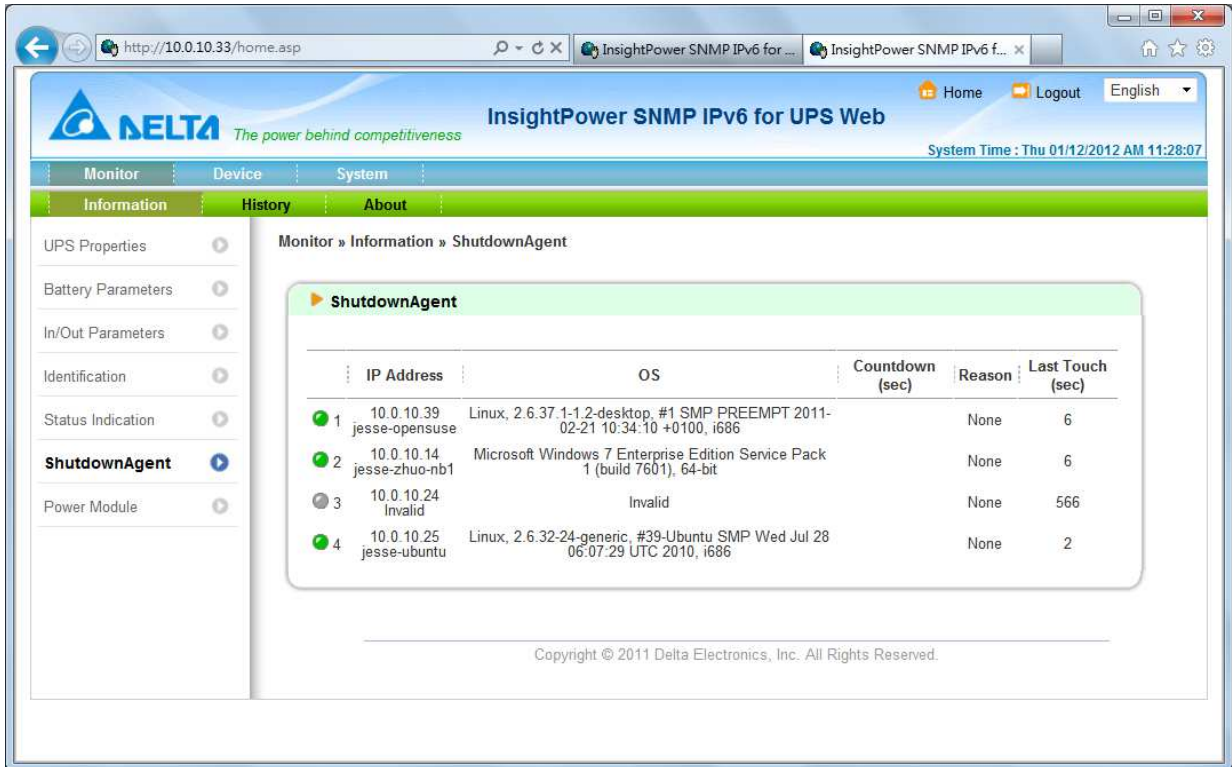
4. Open the ShutdownAgent property from Windows task bar to get the IP address of the server.



5. Back to the InsightPower SNMP IPv6 card web page, add the IP address of ShutdownAgent to the SNMP Trap table. Please select the "ShutdownAgent 2012" for the Event Level and UPSV4 or UPSv5 as the Trap MIB.



6. If you enable the manageable option in the ShutdownAgent then you can observe all of the shutdown status, countdown timer and shutdown reason from the InsightPower SNMP IPv6 card. The web page is on the Monitor >> Information >> ShutdownAgent.



The screenshot shows a web browser window displaying the 'InsightPower SNMP IPv6 for UPS Web' interface. The browser's address bar shows 'http://10.0.10.33/home.asp'. The page has a blue header with the Delta logo and the text 'The power behind competitiveness'. Below the header, there are navigation tabs: 'Monitor', 'Device', 'System', 'Information', 'History', and 'About'. The 'Monitor' tab is selected, and the 'Information' sub-tab is active. The main content area is titled 'Monitor » Information » ShutdownAgent'. It features a table with four columns: 'IP Address', 'OS', 'Countdown (sec)', 'Reason', and 'Last Touch (sec)'. The table lists four entries, each with a status icon (green circle with a checkmark or a grey circle with an 'X'). The first two entries are for Linux and Windows systems, both with a countdown of 6 seconds. The third entry is for an 'Invalid' system with a countdown of 566 seconds. The fourth entry is for a Linux system with a countdown of 2 seconds. The footer of the page contains the copyright notice: 'Copyright © 2011 Delta Electronics, Inc. All Rights Reserved.'

	IP Address	OS	Countdown (sec)	Reason	Last Touch (sec)
1	10.0.10.39 jesse-opensuse	Linux, 2.6.37.1-1.2-desktop, #1 SMP PREEMPT 2011-02-21 10:34:10 +0100, i686		None	6
2	10.0.10.14 jesse-zhuo-nb1	Microsoft Windows 7 Enterprise Edition Service Pack 1 (build 7601), 64-bit		None	6
3	10.0.10.24 Invalid	Invalid		None	566
4	10.0.10.25 jesse-ubuntu	Linux, 2.6.32-24-generic, #39-Ubuntu SMP Wed Jul 28 06:07:29 UTC 2010, i686		None	2